

GWGK

Implementing Cisco Voice Gateways and Gatekeepers

Volumes 1 & 2

Version 1.0

Student Guide

CLS Production Services: 06.21.05

Copyright © 2005, Cisco Systems, Inc. All rights reserved.

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



Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

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

Table of Contents

Volume 1

<i>Course Introduction</i>	1
Overview	1
Learner Skills and Knowledge	1
Course Goal and Objectives	2
Course Flow	3
Additional References	4
Cisco Glossary of Terms	4
Your Training Curriculum	5
<i>Function of Gateways and Gatekeepers</i>	1-1
Overview	1-1
Module Objectives	1-1
<i>Reviewing Gateways and Gatekeepers</i>	1-3
Overview	1-3
Objectives	1-3
Gateways	1-4
Example: Simple Multisite IP Telephony Network	1-6
Gatekeepers	1-7
Deployment Models	1-10
Single-Site Call-Processing Model	1-11
Centralized Call-Processing Model	1-12
Multisite Distributed Call-Processing Model	1-13
Introduction to IP-to-IP Gateways	1-15
Summary	1-16
Lesson Self-Check	1-17
Lesson Self-Check Answer Key	1-18
<i>Selecting a Gateway Protocol</i>	1-19
Overview	1-19
Objectives	1-19
Overview of H.323 Gateways	1-20
H.323 Call Flow	1-23
Overview of MGCP Gateways	1-24
MGCP Call Flow	1-26
Overview of SIP Gateways	1-30
SIP Call Flow	1-34
DTMF Relay Considerations	1-53
Choosing a Gateway Protocol	1-66
Lesson Self-Check	1-71
Lesson Self-Check Answer Key	1-76
<i>Implementing Gateways</i>	1-77
Overview	1-77
Objectives	1-77
H.323 Gateway Integration with Cisco CallManager	1-78
H.323 Gateway Integration with Toll Bypass	1-84
MGCP Gateway Integration with Cisco CallManager	1-87
MGCP Backhauling	1-89
Implementing a SIP Gateway	1-92
SIP Gateway Integration with Cisco CallManager	1-97
Summary	1-99
Lesson Self-Check	1-100
Lesson Self-Check Answer Key	1-102

Configuring Fax and Modem Support **1-103**

Overview	1-103
Objectives	1-103
Fax Relay	1-104
Fax Pass-Through	1-123
Fax Configuration Best Practices	1-132
Modem Relay	1-134
Modem Pass-Through	1-140
Modem Configuration Best Practices	1-143
Summary	1-146
Lesson Self-Check	1-147
Lesson Self-Check Answer Key	1-149
Module Summary	1-150
References	1-150

Integrating a VoIP Network to the PSTN and PBXs **2-1**

Overview	2-1
Module Objectives	2-1

Connecting to the PSTN and PBXs **2-3**

Overview	2-3
Objectives	2-3
Overview of PSTN and PBX Circuit Options	2-4
PSTN and PBX Integration Overview	2-7
PSTN and PBX Integration Requirements	2-9
Analog Integration Characteristics	2-10
Digital Integration Characteristics	2-12
PBX Integration Considerations	2-13
Summary	2-14
Lesson Self-Check	2-15
Lesson Self-Check Answer key	2-17

Analog Circuits **2-19**

Overview	2-19
Objectives	2-19
Analog Signaling Interfaces	2-20
Analog Call Features	2-21
Router Analog Hardware Types	2-25
High-Density Analog	2-27
Analog Trunk Configuration	2-38
Common Analog Issues	2-49
Troubleshooting Tools	2-56
Lesson Self-Check	2-67
Lesson Self-Check Answer Key	2-69

CAS Circuits **2-71**

Overview	2-71
Objectives	2-71
Channel Associated Signaling	2-72
T1 CAS Signaling	2-73
E1 R2	2-79
CAS Configuration	2-84
Troubleshooting CAS Circuits	2-91
Summary	2-98
Lesson Self-Check	2-99
Lesson Self-Check Answer Key	2-101

ISDN PRI Circuits **2-103**

Overview	2-103
Objectives	2-103
ISDN Circuit Review	2-104
Network Side vs. User Side	2-106
ISDN Signaling	2-107
ISDN IEs	2-109
Example: IE in Action	2-111
ISDN Numbering Plan	2-119
Common ISDN Implementation Requirements	2-121
Calling Name Display	2-127
Common ISDN Gateway Configuration Examples	2-128
Troubleshooting ISDN Circuits	2-138
Summary	2-156
Lesson Self-Check	2-157
Lesson Self-Check Answer Key	2-159

QSIG Integration **2-161**

Overview	2-161
Objectives	2-161
QSIG Circuit Overview	2-162
QSIG Signaling	2-164
Common QSIG Implementation Considerations	2-165
Common QSIG Gateway Configuration Examples	2-171
Troubleshooting QSIG Circuits	2-175
Summary	2-177
Lesson Self-Check	2-178
Lesson Self-Check Answer Key	2-179
Module Summary	2-180
References	2-180

Volume 2

Implementing Dial Plans **3-1**

Overview	3-1
Module Objectives	3-1

Dial Plan Overview **3-3**

Overview	3-3
Objectives	3-3
Introducing Numbering and Dial Plans	3-4
Numbering Plans	3-6
Designing a Scaleable Dial Plan	3-8
Overlapping Dial Plans	3-14
Summary	3-16
References	3-16
Lesson Self-Check	3-17
Lesson Self-Check Answer Key	3-18

Digit Manipulation **3-19**

Overview	3-19
Objectives	3-19
Defining Digit Manipulation	3-20
Matching Inbound and Outbound Digits	3-21
Using Prefixes and No-Digit Stripping	3-24
Using Number Expansion	3-26
Using CLID	3-28

Manipulating ANI and DNIS	3-31
Translation Rule Regular Expressions	3-33
Configuring Translation Rules	3-35
Manipulating Numbering Plan Types	3-38
Troubleshooting Translation Rules	3-39
Order of Operation in Digit Manipulation	3-41
Summary	3-42
References	3-42
Lesson Self-Check	3-43
Lesson Self-Check Answer Key	3-44
<i>Class of Restrictions</i>	3-45
Overview	3-45
Objectives	3-45
COR Overview	3-46
COR Operation	3-48
COR vs. Cisco CallManager	3-51
Configuring COR	3-53
Verifying COR	3-57
Summary	3-59
References	3-59
Lesson Self-Check	3-60
Lesson Self-Check Answer Key	3-62
<i>Influencing Call Routes</i>	3-63
Overview	3-63
Objectives	3-63
Influencing Call Routes	3-64
Hunt Groups	3-65
Manipulating Cause Codes	3-67
Tail-End Hop-Off	3-68
Call Admission Control	3-69
Types of CAC	3-72
Local CAC Mechanisms	3-73
Measurement-Based CAC Mechanisms	3-75
Resource-Based CAC Mechanisms	3-86
Evaluating CAC Mechanisms	3-98
Summary	3-100
References	3-100
Lesson Self-Check	3-101
Lesson Self-Check Answer Key	3-102
Module Summary	3-103
References	3-103
<i>Implementing Advanced Gateway Features</i>	4-1
Overview	4-1
Module Objectives	4-1
<i>Deploying SRST</i>	4-3
Overview	4-3
Objectives	4-3
SRST Overview	4-4
SRST Dial Plan	4-7
Configuring SRST	4-12
Implementing SRST Features	4-17
Troubleshooting SRST	4-35
Summary	4-36
References	4-36
Lesson Self-Check	4-37

Lesson Self-Check Answer Key	4-38
<i>Digital Signal Processors in Gateways</i>	4-39
Overview	4-39
Objectives	4-39
DSP Overview	4-40
Codec Complexity	4-50
DSP Farm Overview	4-56
DSP Design Considerations	4-58
Configuring DSPs on a Gateways	4-65
Summary	4-74
References	4-74
Lesson Self-Check	4-76
Lesson Self-Check Answer Key	4-78
<i>Toolkit Command Language</i>	4-79
Overview	4-79
Objectives	4-79
Toolkit Command Language	4-80
Applying TCL Scripts	4-90
Verifying TCL Scripts	4-105
Summary	4-107
References	4-107
Lesson Self-Check	4-108
Lesson Self-Check Answer Key	4-110
Module Summary	4-111
References	4-111
<i>Deploying Gatekeepers</i>	5-1
Overview	5-1
Module Objectives	5-1
<i>Cisco Gatekeeper Overview</i>	5-3
Overview	5-3
Objectives	5-3
Gatekeeper Overview	5-4
Deployment Scenarios	5-7
Gatekeeper Hardware and Software Requirements	5-8
Gatekeeper Signaling	5-10
Zones and Zone Prefixes	5-37
Technology Prefixes	5-40
H.323 Proxy Functions	5-43
Gatekeeper Transaction Message Protocol	5-46
Gatekeeper Address Resolution Process	5-47
Summary	5-49
References	5-50
Lesson Self-Check	5-51
Lesson Self-Check Answer Key	5-53
<i>Configuring Gatekeepers</i>	5-55
Overview	5-55
Objectives	5-55
Basic Gatekeeper Configuration	5-56
Configuring Endpoints for Gatekeeper Support	5-58
Implementing Gatekeeper Zones	5-62
Implementing Gatekeeper CAC	5-67
Configuring Gatekeeper-Controlled Trunks	5-70
Troubleshooting Gatekeepers	5-80
Summary	5-83

References	5-83
Lesson Self-Check	5-84
Lesson Self-Check Answer Key	5-85
<i>Configuring Directory Gatekeepers</i>	<i>5-87</i>
Overview	5-87
Objectives	5-87
Directory Gatekeeper Overview	5-88
Directory Gatekeeper Signaling	5-91
Configuring Directory Gatekeepers	5-93
Troubleshooting Directory Gatekeepers	5-96
Summary	5-102
References	5-102
Lesson Self-Check	5-103
Lesson Self-Check Answer Key	5-104
<i>Configuring Gatekeeper Redundancy</i>	<i>5-105</i>
Overview	5-105
Objectives	5-105
Gatekeeper Redundancy Overview	5-106
Deploying Gatekeepers using HSRP	5-107
Implementing Alternate Gatekeepers	5-110
Implementing GUP	5-112
Implementing Gatekeeper Clustering	5-114
Summary	5-122
Lesson Self-Check	5-123
Lesson Self-Check Answer Key	5-124
Module Summary	5-125
References	5-125

<i>Introducing Service Provider Offerings</i>	6-1
Overview	6-1
Module Objectives	6-1
<i>Understanding Service Provider Offerings</i>	6-3
Overview	6-3
Objectives	6-3
Service Provider Offerings	6-4
IP Centrex	6-9
IP PSTN	6-10
Residential VoIP	6-11
Calling Card Services	6-12
Wholesale Voice Services	6-14
Summary	6-15
Lesson Self-Check	6-16
Lesson Self-Check Answer Key	6-17
<i>Cisco Multiservice IP-to-IP Gateway</i>	6-19
Overview	6-19
Objectives	6-19
Cisco Multiservice IP-to-IP Gateway Overview	6-20
Cisco Multiservice IP-to-IP Gateway and Gatekeeper Design	6-24
Cisco Multiservice IP-to-IP Gateway Signaling	6-31
Cisco Multiservice IP-to-IP Gateways Integration with a Service Provider and Cisco CallManager	6-37
Cisco Multiservice IP-to-IP Gateways Fax, Modem, and DTMF Considerations	6-41
Cisco Multiservice IP-to-IP Gateway Configuration	6-42
Summary	6-43
References	6-43
Lesson Self-Check	6-44
Lesson Self-Check Answer Key	6-45
Module Summary	6-46
References	6-46

Course Introduction

Overview

Implementing Cisco Voice Gateways and Gatekeepers (GWGK) v1.0 provides network administrators and network engineers with the knowledge and skills required to integrate gateways and gatekeepers into an enterprise VoIP network. This course is one of several courses in the CCVP track that addresses design, planning, and deployment practices and provides comprehensive hands-on experience in configuration and deployment.

Learner Skills and Knowledge

This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should complete in order to benefit fully from this course.

Learner Skills and Knowledge

Cisco.com

- **CCNP® Network Support or CCDP® Network Design**
- **Implementing Cisco Quality of Service (QoS)**
- **Cisco Voice over IP (CVOICE)**
- **Cisco IP Telephony (CIPT) Parts 1 and 2**
- **Cisco IP Telephony Express (IPTX)**
- **Cisco IP Telephony Troubleshooting (IPTT)**
- **PBX Technology Concepts**
- **Cisco Unity and Voice-Mail Systems Concepts**

Course Goal and Objectives

This topic describes the course goal and objectives.

Course Goal

Cisco.com

“To provide network administrators and network engineers with the knowledge and skills required to integrate gateways and gatekeepers into an enterprise VOIP network.”

Implementing Cisco Voice Gateways and Gatekeepers

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

Upon completing this course, you will be able to meet these objectives:

- Describe the function of gateways and gatekeepers in a VoIP environment that includes H.323, MGCP, and SIP protocols
- Identify the requirements for integrating a VoIP network with the PSTN and PBXs using voice gateways
- Implement a dial plan on a Cisco gateway by using dial plans, number plans, and COR applications
- Configure advanced voice gateway features
- Implement gatekeepers and directory gatekeepers in an H.323 VoIP environment
- Describe common service provider offerings such as wholesale voice and IP Centrex and describe how an IP-to-IP gateway supports these offerings

Course Flow

This topic presents the suggested flow of the course materials.

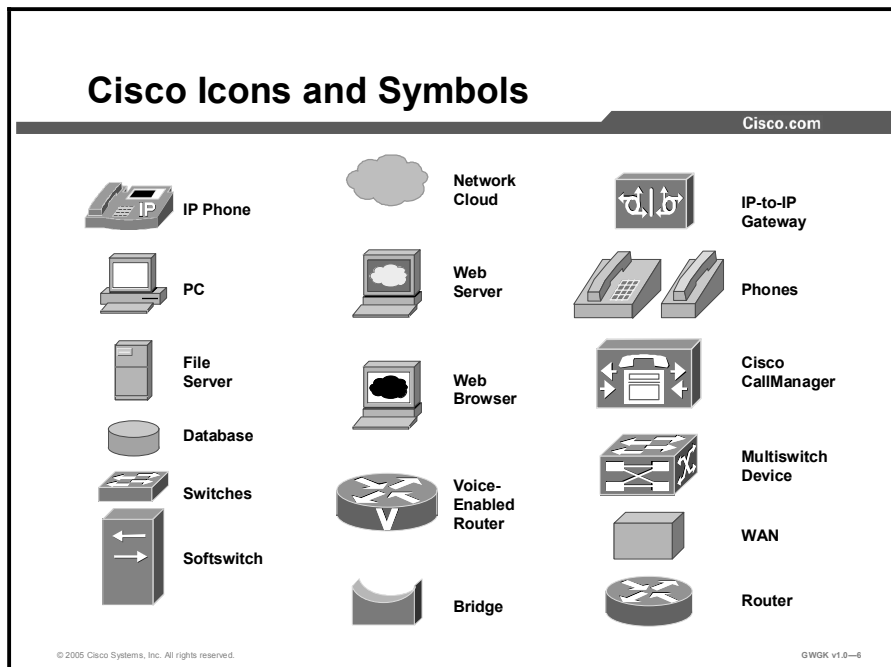
		Course Flow				
		Cisco.com				
		Day 1	Day 2	Day 3	Day 4	Day 5
A M		Course Introduction	Configuring PSTN Connections	Implementing Advanced Gateway Features	Deploying Gatekeepers	Comprehensive Lab
		Functions of Gateways and Gatekeepers	Implementing a Dial Plan		Configuring Gatekeepers	
					Configuring Directory Gatekeepers	
Lunch						
P M		Configuring MGCP Gateways	Implementing a Dial Plan and COR	Configuring SRST	Introducing Service Provider Offerings	
		Integrating a VoIP Network to the PSTN and PBXs		Configuring DSP Farms		
				Configuring TCL Scripts		

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-5

The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

Additional References

This topic presents the Cisco icons and symbols used in this course, as well as information on where to find additional technical references.



Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>.

Your Training Curriculum

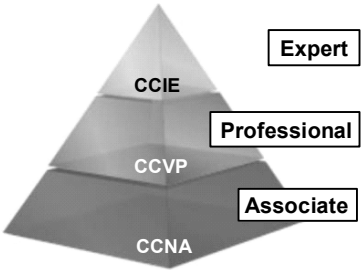
This topic presents the training curriculum for this course.

Cisco Voice Career Certifications

Cisco.com

Expand Your Professional Options and Advance Your Career CCVP

Professional-level recognition in voice



Required Exam	Recommended Training Through Cisco Learning Partners
642-452	Implementing Cisco Voice Gateways and Gatekeepers (GWGK)
642-443	Cisco IP Telephony Part 1 (CIPT1) Cisco IP Telephony Part 2 (CIPT2)
642-642	Implementing Quality of Service (QoS)
642-432	Cisco Voice over IP (CVOICE)
642-425	Cisco IP Telephony Troubleshooting (IPTT)

<http://www.cisco.com/go/certifications>

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-7

You are encouraged to join the Cisco Certification Community, a discussion forum open to anyone holding a valid Cisco Career Certification (such as Cisco CCIE[®], CCNA[®], CCDA[®], CCNP[®], CCDP[®], CCIP[®], or CCSP[®]). It provides a gathering place for Cisco-certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit http://www.cisco.com/en/US/learning/le3/le2/le41/learning_certification_level_home.html.

Module 1

Function of Gateways and Gatekeepers

Overview

Organizations that migrate to IP telephony install gateways to connect networks, such as their LAN and the public switched telephone network (PSTN), or to connect their new IP telephony network segments and a PBX that supports the remaining traditional telephony network. Organizations install gatekeepers to simplify routing between voice gateways and for call admission control.

If you are responsible for implementing or operating a gateway, you need to know which gateway protocol best suits your situation and how to configure it properly. This module introduces the function of H.323, Media Gateway Control Protocol (MGCP), and Session Initiation Protocol (SIP) gateways in an IP telephony environment. Although gatekeepers are discussed briefly, most of the module concerns gateways. You will learn about gatekeepers in the module “Deploying Gatekeepers.”

Module Objectives

Upon completing this module, you will be able to describe the function of gateways and gatekeepers in a VoIP environment that includes H.323, MGCP, and SIP protocols. This ability includes being able to meet these objectives:

- Explain the placement and function of gateways and gatekeepers in a network
- Evaluate voice gateway protocols to ensure that the best protocol of H.323, MGCP, or SIP is implemented at various sites in a network
- Explain the problems with implementing voice gateways in support of IP telephony solutions
- Explain how fax traffic and modem traffic are supported on an H.323, an MGCP, and a SIP gateway

Lesson 1

Reviewing Gateways and Gatekeepers

Overview

This lesson is the first step in helping learners to develop expertise in evaluating gateway and gatekeeper issues in an IP telephony implementation. It introduces a scenario that will be used throughout the course to provide context for situations that learners may encounter in their own networks.

Objectives

Upon completing this lesson, you will be able to explain the placement and function of gateways and gatekeepers in a network. This ability includes being able to meet these objectives:

- Describe the role and functionality of Cisco gateways
- Describe the role and functionality of Cisco gatekeepers
- Describe the three Cisco CallManager deployment models
- Determine the placement and function of a gateway in a single-site call processing model
- Determine the placement and function of a gateway in a centralized call processing model
- Determine the placement and function of gateways and gatekeepers in a multisite distributed call processing model
- Describe the functions of IP-to-IP gateways

Gateways

This topic describes the role and function of Cisco gateways.

Cisco Gateway Role in IP Telephony

Cisco.com

- **The voice gateway connects an IP telephony network to the PSTN or to a PBX.**
- **Specifically, its role is the following:**
 - **Convert IP telephony packets into analog or digital signals**
 - **Connect an IP telephony network to analog or digital trunks or to individual analog stations**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0--1.3

A voice gateway allows terminals of one type, such as H.323, to communicate with terminals of another type, such as a PBX, by converting protocols. Gateways connect a company network to the public switched telephone network (PSTN), a PBX, or individual analog devices such as a phone or fax. Gateways range from specialized, entry-level and standalone voice gateways, to high-end, feature-rich integrated routers and Cisco Catalyst software gateways.

These are the two types of Cisco access gateways:

- **Analog gateways:** There are two categories of Cisco access analog gateways:
 - Analog station gateways connect an IP telephony network to plain old telephone service (POTS). They provide Foreign Exchange Station (FXS) ports for connecting to analog telephones, interactive voice response (IVR) systems, fax machines, and voice-mail systems.
 - Analog trunk gateways connect an IP telephony network to the PSTN central office (CO) or a PBX. They provide Foreign Exchange Office (FXO) ports for PSTN or PBX access and recEive and transMit (E&M) ports for analog trunk connection to a legacy PBX. To minimize any answer and disconnect supervision issues, use digital gateways whenever possible. Analog Direct Inward Dial (DID) is also available for PSTN connectivity.
- **Digital Gateways:** Cisco access digital trunk gateways connect an IP telephony network to the PSTN or to a PBX via digital trunks, such as PRI common channel signaling (CCS), BRI, T1 channel-associated signaling (CAS), or E1. Digital T1 PRI trunks may also connect to certain legacy voice-mail systems.

Cisco Gateway Functions

Cisco.com

- **Serve gateway protocols**
 - H.323
 - SIP
 - MGCP
- **Provide core gateway requirements**
 - DTMF relay
 - Supplementary services
 - Cisco CallManager redundancy
- **Enable call survivability**
- **Provide TDM interface to a PBX and the PSTN**
- **Provide fax or modem, or both**

© 2005 Cisco Systems, Inc. All rights reserved.

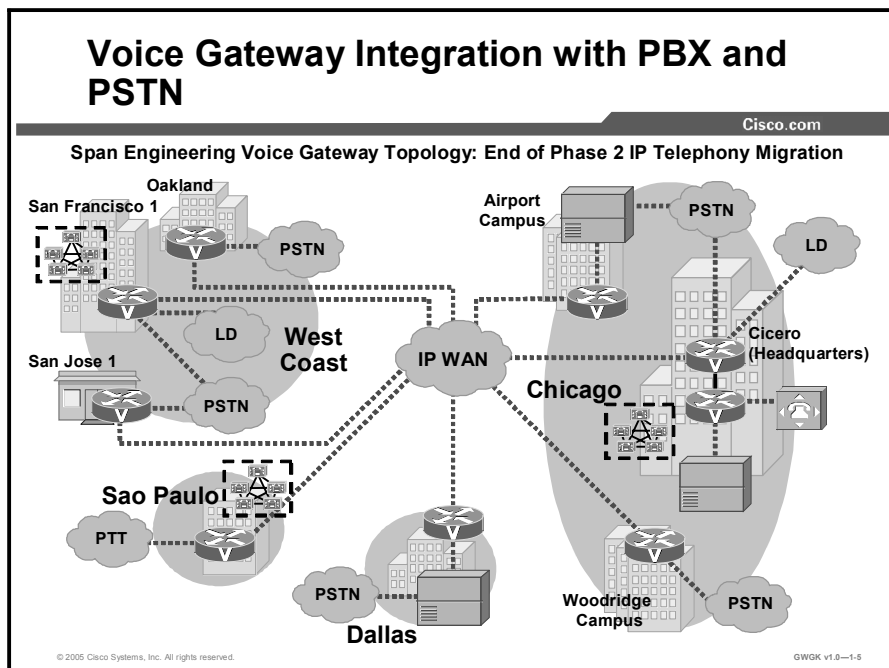
GWGK v1.0-1.4

IP telephony gateways must meet these core feature requirements:

- **Gateway protocol support:** Gateways support H.323, Media Control Gateway Protocol (MGCP), and Session Initiation Protocol (SIP). H.323 and SIP can be deployed on networks in which a call control agent, such as Cisco CallManager, is not present. MGCP is a streamlined protocol and only works on a network in which a Cisco CallManager is present.
- **Core gateway requirements:** These are the three core gateway requirements:
 - **Dual tone multi-frequency (DTMF) relay capabilities:** Each digit dialed with tone dialing is assigned a unique pair of frequencies. Voice compression of these tones with a low bit-rate codec can cause DTMF signal loss or distortion. Therefore, DTMF tones are separated from the voice bearer stream and sent as signaling indications through the gateway protocol (H.323, SCCP, or MGCP) signaling channel instead.
 - **Supplementary services support:** These services provide user functions such as hold, transfer, and conferencing and are considered fundamental requirements of any voice installation.
 - **Cisco CallManager redundancy support:** The gateways must support the ability to “rehome” to a secondary Cisco CallManager in the event of a primary Cisco CallManager failure.
- **Call survivability in Cisco CallManager:** The voice gateway preserves the Real-Time Transport Protocol (RTP) bearer stream (the voice conversation) between two IP endpoints when the Cisco CallManager to which the endpoint is registered is no longer reachable.
- **Q Signaling (QSIG) support:** QSIG is becoming the standard for PBX interoperability in Europe and North America. With QSIG, the Cisco voice packet network appears to PBXs as a distributed transit PBX that can establish calls to any PBX or other telephony endpoint served by a Cisco gateway, including non-QSIG endpoints.
- **Fax and modem support:** Fax over IP enables interoperability of traditional analog fax machines with IP telephony networks. The fax image is converted from an analog signal and is carried as digital data over the packet network.

Example: Simple Multisite IP Telephony Network

Span Engineering LLC, a fictitious company that is migrating to a Cisco IP telephony solution, has three sites in the United States and a fourth site in Brazil. The figure shows gateway deployment, following a partial migration to IP telephony, in an organizational setting.



Span Engineering is a U.S.-based company with headquarters in Chicago. It has branches in Dallas and on the West Coast in the Bay Area and has recently expanded internationally to Sao Paulo, Brazil. The company is carrying out a phased migration to IP telephony, described in the following three phases.

- **Phase 1:** Toll bypass between Dallas and Chicago and between Chicago-area campuses.
- **Phase 2:** Span Engineering deploys Cisco CallManager in Chicago, the West Coast, Dallas, and Sao Paulo. Some locations are migrated to IP telephony; some remain on the PBX as shown in the figure. This migration occurs immediately following toll bypass implementation.
- **Phase 3:** Migration to IP telephony is completed and the remaining PBXs are taken out of the network.

You will be using Span Engineering throughout this course as an example to help you consider gateway implementations.

Gatekeepers

This topic describes the role and function of a Cisco gatekeeper.

Cisco Gatekeeper Role and Functions

Cisco.com

Gatekeepers enable scalability and call admission and have the following functions:

- **Mandatory gatekeeper functions**
 - Address translation
 - Admission control
 - Bandwidth control
 - Zone management
- **Optional gatekeeper functions**
 - Call authorization
 - Call management
 - Bandwidth management
 - Call control signaling

© 2005 Cisco Systems, Inc. All rights reserved. GWOK v1.0-1.6

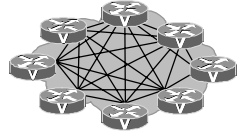
A gatekeeper is an H.323 LAN device. It has the following functions:

- **Mandatory Gatekeeper Functions**
 - **Address Translation:** A gatekeeper translates H.323 IDs and standard E.164 telephone numbers to endpoint IP addresses.
 - **Admission Control:** Controls endpoint admission into the H.323 network. To achieve this, the gatekeeper uses H.225 Registration, Admission, and Status (RAS) messages and Admission Request (ARQ), Admission Confirmation (ACF), and Admission Rejection (ARJ) messages.
 - **Bandwidth Control:** Gatekeepers use H.225 Bandwidth Request (BRQ), Bandwidth Confirmation (BCF), and Bandwidth Rejection (BRJ) messages to manage endpoint bandwidth requirements.
 - **Zone Management:** The gatekeeper manages all registered endpoints in the zone.
- **Optional Gatekeeper Functions**
 - **Call Authorization:** With this option, the gatekeeper can restrict access to certain terminals or gateways or 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:** Gatekeepers route call-signaling messages between H.323 endpoints using the gatekeeper routed call-signaling (GKRCS) model. It may also allow endpoints to send H.225 call-signaling messages directly to each other.

IP Telephony Network Scalability

Cisco.com

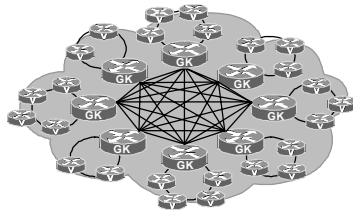
Small Network—Gateways Only



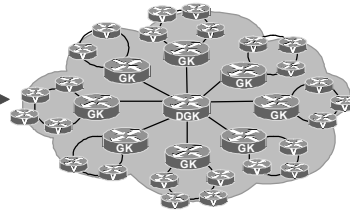
Small Network—Simplified with a Gatekeeper



Medium Network—Multiple Gatekeepers



Medium to Large Network—Multiple Gatekeepers and a Directory Gatekeeper



© 2005 Cisco Systems, Inc. All rights reserved.

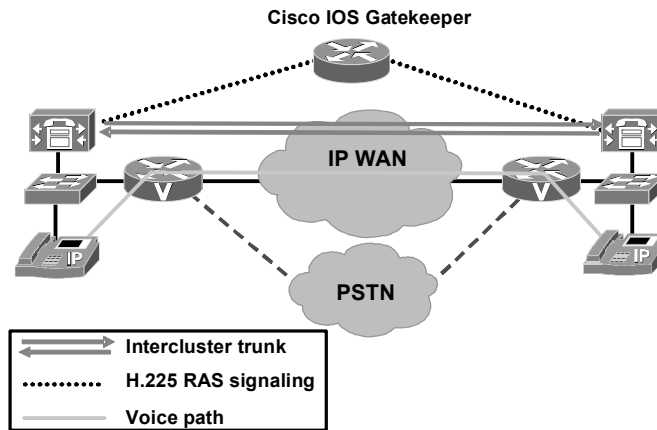
GWGK v1.0-1.7

Gateways are responsible for edge routing decisions between the PSTN and the H.323 network. Cisco gatekeepers are used to group gateways into logical zones and perform call routing between them. Cisco gatekeepers handle the core call routing among devices in the H.323 network and provide centralized dial plan administration. Without a Cisco gatekeeper, explicit IP addresses for each terminating gateway would have to be configured at the originating gateway and matched to a VoIP dial peer, shown as a “Small Network—Gateways Only” in the figure. With a Cisco gatekeeper, gateways query the gatekeeper when trying to establish VoIP calls with remote VoIP gateways, shown as a “Small Network— Simplified” with a gatekeeper in the figure.

The figure illustrates the concept of VoIP network scaling with gatekeepers and directory gatekeepers. In the case of the small network, a single gatekeeper adds scalability to the network when the network evolves into a larger network and subsequently requires a directory gatekeeper to make the network more manageable.

Call Admission Control

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-8

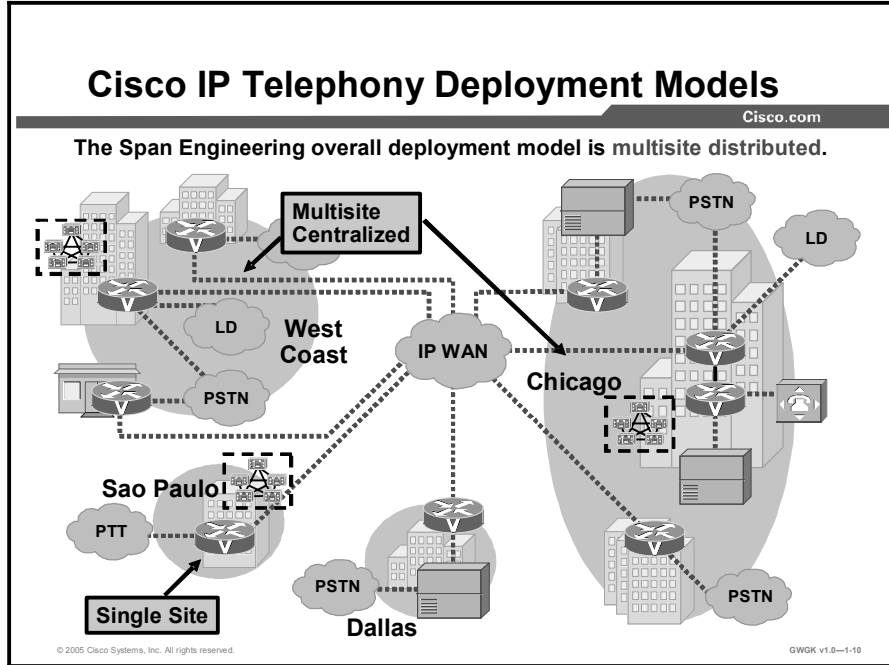
The value of the gatekeeper for network scalability through zone management is further enhanced by what it does for Call Admission Control (CAC).

A gatekeeper device provides CAC for distributed call-processing systems. In a distributed system, each site contains its own call-processing capability. For example, the figure shows two sites, each with its own Cisco CallManager connected by an IP WAN link. A gatekeeper provides CAC over the IP WAN link in this example by using the H.225 RAS protocol message set that is used for CAC, bandwidth allocation, and dial pattern resolution (call routing). The gatekeeper provides these services for communications between Cisco CallManager clusters and H.323 networks.

An intercluster trunk is an H.323 connection that allows two Cisco CallManager clusters to be connected over an IP WAN. Use intercluster trunks when you are routing intercluster calls across a remote WAN link.

Deployment Models

This topic describes three Cisco CallManager deployment models.



There are three primary Cisco CallManager deployment models: A single location, multiple locations with a single Cisco CallManager cluster, or multiple locations with Cisco CallManager clusters at each location. Regardless of the deployment model, if a company has multiple sites that are distant from each other, for instance, each site is served by a different public safety answering point (PSAP) for emergency services, gateways are required at each site.

The single-site model consists of a call processing agent located at a single site such as a building or small campus. Voice traffic is carried throughout the site by a LAN or metropolitan-area network (MAN). Calls beyond the LAN or MAN use the public switched telephone network (PSTN). No telephony services are provided over the WAN.

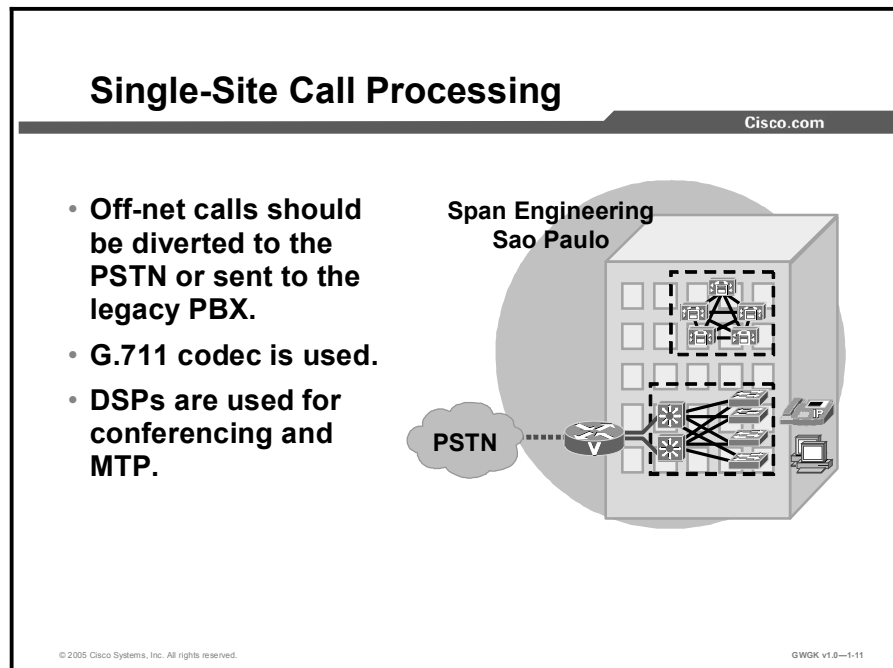
The multisite WAN model with centralized call processing consists of a single call-processing agent that provides services for many sites and uses the IP WAN to transport voice traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites.

The multisite WAN model with distributed call processing consists of multiple independent sites, each with its own call-processing agent connected to an IP WAN that carries voice traffic between the distributed sites. The IP WAN in this model does not carry call control signaling between the sites because each site has its own call-processing agent.

Clustering over the IP WAN (multisite single distributed cluster) deploys a single Cisco CallManager cluster across multiple sites that are connected by an IP WAN with quality of service (QoS) features enabled.

Single-Site Call-Processing Model

This topic describes the placement and function of a gateway in a single-site call-processing model.



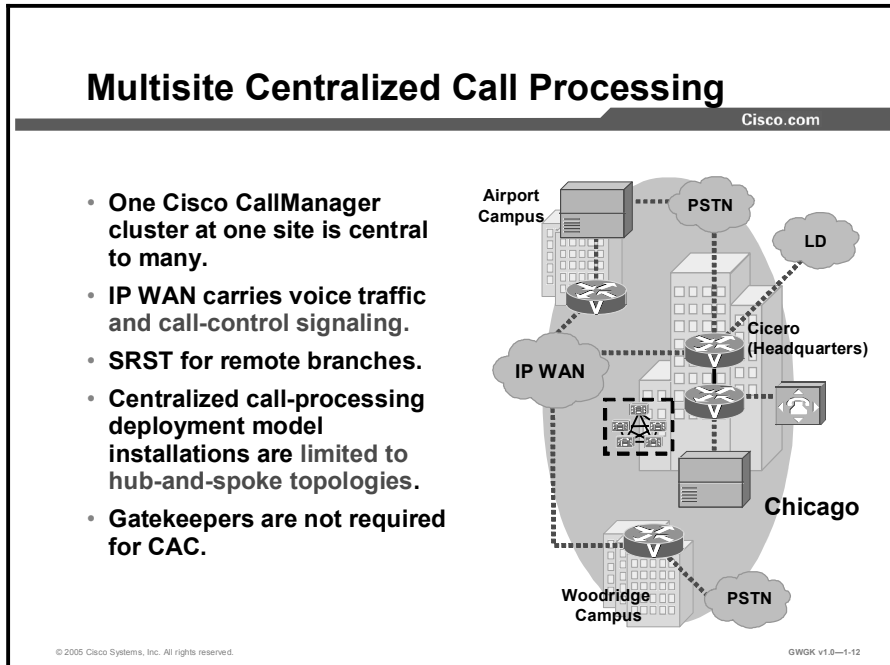
In a geographically distributed network undergoing migration to IP telephony, each location can be considered a single site. A location that originally is identified as a single site might not be considered a single site after all of the facilities in the area have been migrated. Consequently, a single-site call-processing model can be a complex mix where PSTN, PBX, and IP telephony coexist.

These are the issues specific to voice gateways for the single-site deployment model:

- Use G.711 codecs so digital signal processors (DSPs) are not required for transcoding and can be allocated to other functions such as conferencing and Media Termination Points (MTPs).
- Use MGCP gateways for the PSTN if H.323 functionality is not required. This simplifies the dial plan configuration. H.323 might be required to support specific functionality not offered with MGCP, such as support for Signaling System 7 (SS7) or Non-Facility Associated Signaling (NFAS).
- Gatekeepers are not required since there is a single, highly available voice gateway that connects to the PSTN.

Centralized Call-Processing Model

This topic describes the placement and function of a gateway in a centralized call-processing model.



When a company has several remote sites, it can choose to centralize the call-processing agent in a single location that services all the remote sites.

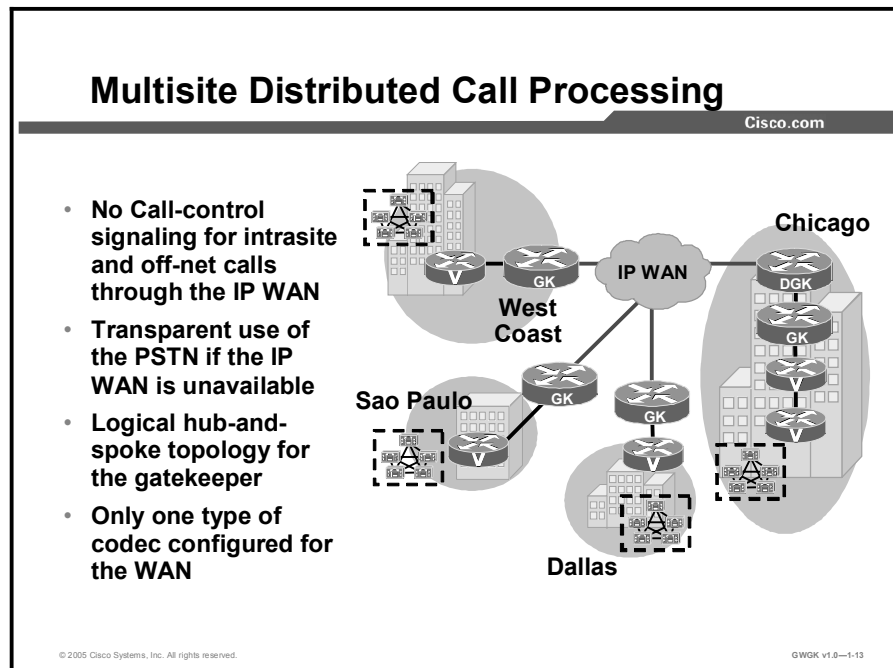
The multisite WAN model with centralized call processing consists of a single call-processing agent that provides services for many sites and uses the IP WAN to transport voice traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites.

A variety of Cisco gateways can provide the remote sites with PSTN access. When the IP WAN is down, or if all the available bandwidth on the IP WAN has been consumed, users at the remote sites can dial the PSTN access code and place their calls through the PSTN. The Cisco Survivable Remote Site Telephony (SRST) feature, available on Cisco IOS gateways, provides call processing at the branch offices in the event of a WAN failure.

If there are many remote sites, each with a gateway, you can improve the performance of the network by adding a gatekeeper for scalability, manageability, and dial-plan resolution. A gatekeeper is not required for CAC since there are no intercluster trunks involved in this deployment.

Multisite Distributed Call-Processing Model

This topic describes the placement and function of gateways and gatekeepers in a multisite distributed call-processing model.



When a company has several remote sites, instead of centralizing its call processing agents in a single location, it can put them in multiple locations. This model saves on call overhead and impacts the QoS of the IP telephony network.

Multisite distributed call processing allows each site to be completely self-contained. In the event of an IP WAN failure or insufficient bandwidth, the site does not lose call-processing service or functionality. Cisco CallManager simply sends all calls between the sites across the PSTN.

Each site in the distributed call-processing model can be one of the following:

- A single site with its own call processing agent, which can be either:
 - Cisco CallManager
 - Cisco CallManager Express
 - Other IP PBX
- A centralized call processing site and all of its associated remote sites
- A legacy PBX with a VoIP gateway

An IP WAN interconnects all the distributed call-processing sites. Typically, the PSTN serves as a backup connection between the sites in case the IP WAN connection fails or does not have any more available bandwidth. A site connected only through the PSTN is a standalone site and is not covered by the distributed call-processing model.

Gatekeepers are one of the key elements in the multisite WAN model with distributed call processing. Each gatekeeper provides dial-plan resolution and CAC. The following best practices apply to the use of a gatekeeper:

- Use a logical hub-and-spoke topology for the gatekeeper. A gatekeeper can manage the bandwidth into and out of a site, or between zones within a site, but it is not aware of the topology.
- Size the platforms appropriately to ensure that performance and capacity requirements can be met.
- When deploying voice in a WAN environment, Cisco recommends that you use the lower-bandwidth G.729 codec for any voice calls that will traverse WAN links because this practice will provide bandwidth savings on these lower-speed links.
- Gatekeeper networks can scale to hundreds of sites, and the design is limited only by the hub-and-spoke topology.

For distributed call-processing systems, you can implement CAC with an H.323 gatekeeper. In this design, the call-processing agent registers with the gatekeeper and queries it each time the agent wants to place an IP WAN call. The gatekeeper associates each call-processing agent with a zone that has specific bandwidth limitations. Thus, the gatekeeper can limit the maximum amount of bandwidth consumed by IP WAN voice calls into or out of a zone.

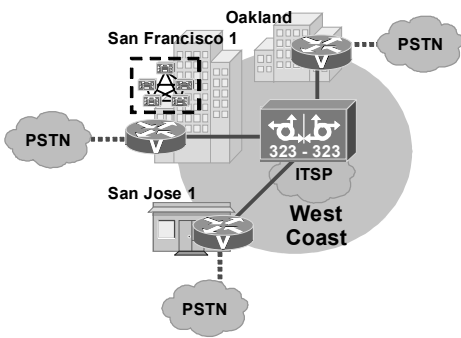
Introduction to IP-to-IP Gateways

This topic describes the role and functions of IP-to-IP gateways.

The IP-to-IP Gateway

Cisco.com

- **IP-to-IP Gateway joins two IP call legs, a PSTN and an IP call leg.**
- **IP-to-IP Gateway supports T.38 fax relay.**
- **Avoid installing voice network modules in any router that will operate as an IP-to-IP Gateway.**



© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-1.14

The Cisco Multiservice IP-to-IP Gateway provides a mechanism to enable H.323 VoIP and videoconferencing calls from one IP network to another. It provides a control point and a demarcation for VoIP and video calls traversing administrative domains. This gateway performs most of the same functions of a PSTN-to-IP gateway, but typically joins two IP call legs, not a PSTN and an IP call leg. Notice in the figure that these calls go through the Internet telephony service provider (ITSP).

The IP-to-IP gateway supports T.38 fax relay. However, endpoints configured with Named Signaling Events (NSEs) may result in reduced fax transmission quality and are not supported.

Cisco IP-to-IP gateways do not support time-division multiplexing (TDM) voice in Cisco IOS Release 12.3(4)T images. The IP-to-IP gateway ignores voice network modules installed in the router and does not allow you to create voice ports. Cisco recommends that you avoid installing voice network modules in any router that will operate as an IP-to-IP gateway.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Voice gateways typically connect an IP network to the PSTN and a traditional PBX.**
- **Gatekeepers allow for CAC and scalability in an IP telephony network.**
- **The three basic Cisco IP telephony deployment models that organizations may use are single-site and multisite with either centralized or distributed call processing.**
- **In the single-site deployment model, the Cisco CallManager applications and the DSP resources are at the same physical location. The PSTN handles all external calls.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-1-15

Summary (Cont.)

Cisco.com

- **The multisite centralized model has a single call-processing agent that limits network topologies to hub and spoke. Applications and DSP resources are centralized or distributed. The IP WAN carries voice traffic and call control signaling between sites.**
- **The multisite distributed model has multiple independent sites and each site has a call-processing agent. The IP WAN carries voice traffic between sites but does not carry call control signaling for intrasite calls or local off-net calls.**
- **IP-to-IP gateways perform similar functions to voice gateways except that they connect VoIP links, not PSTN or PBX links.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-1-16

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 response best describes the functions of a voice gateway? (Source: Gateways)
- A) The voice gateway provides standard AAA services to an IP telephony network.
 - B) The voice gateway connects two different types of networks, providing call control services and call routing.
 - C) The voice gateway enables call admission control in a VoIP network.
 - D) The voice gateway is part of the voice-security platform portfolio, providing a gateway through which only authorized users can get the benefits of such things as toll bypass.
- Q2) A company has four sites. Which of the following IP telephony network situations requires that a gatekeeper coordinate CAC? (Source: Gatekeepers)
- A) A Cisco CallManager is located at one site and the remaining sites are served by voice gateways with SRST.
 - B) A single cluster is distributed over two of the sites and the remaining two sites are served by voice gateways with SRS.
 - C) One site has been converted to IP telephony and the remaining sites are still running traditional telephony.
 - D) Each site has a Cisco CallManager cluster.
- Q3) What is the role of the IP-to-IP gateway in IP telephony? (Source: Introduction to IP-IP Gateways)
-
- Q4) Which response best describes a multisite distributed deployment model?
- A) Several sites supported by a single Cisco CallManager cluster and where call control information is passed over the WAN between sites.
 - B) Several sites, each with a Cisco CallManager cluster. Call control information between sites is passed between sites for intrasite calls and tail-end hop-off calls to the PSTN at a remote site from the calling party location.
 - C) Several sites, each with a Cisco CallManager cluster. The clusters in each location eliminate the requirement for passage of call control information.
 - D) Several sites supported by a single Cisco CallManager cluster that has subscribers and backup servers at different sites from the publisher.

Lesson Self-Check Answer Key

- Q1) B
- Q2) D
- Q3) The IP-to-IP gateway joins two IP call legs, not a PSTN and IP call leg.
- Q4) B

Lesson 2

Selecting a Gateway Protocol

Overview

Customers normally tell you what type of gateway to deploy to support their IP telephony solution. However, because of challenges that may inhibit rapid deployment, you need to be able to fix any problems that arise on any gateway type a customer has chosen. You need to know why a particular gateway type has been chosen and what the potential challenges are in installing it.

This lesson discusses the role of the three gateway protocols, the steps involved in call flow for each, and some issues around dual tone multifrequency (DTMF) and Call Admission Control (CAC), and provides a comparison of the three protocols to help you make a judgment on the suitability of a protocol for specific deployments.

Objectives

Upon completing this lesson, you will be able to evaluate voice gateway protocols to ensure that the best protocol of H.323, MGCP, or SIP is implemented at various sites in a network. This ability includes being able to meet these objectives:

- List the functions performed by a typical H.323 gateway
- Diagram a VoIP call flow entering and leaving a H.323 gateway
- List the functions performed by a typical MGCP gateway
- Diagram a VoIP call flow entering and leaving a MGCP gateway
- List the functions performed by a typical SIP gateway
- Diagram a VoIP call flow entering and leaving a SIP gateway
- Identify the possible issues with DTMF tones in a VoIP network that includes PSTN, PBXs, and H.323 gateways
- Describe the criteria for selecting one gateway protocols over another

Overview of H.323 Gateways

This topic describes the functions of a typical H.323 gateway.

Overview of H.323 Gateways

Cisco.com

H.323 gateways perform the following services:

- **Translation between audio, video, and data formats**
- **Conversion between call setup signals and procedures**
- **Conversion between communication control signals and procedures**

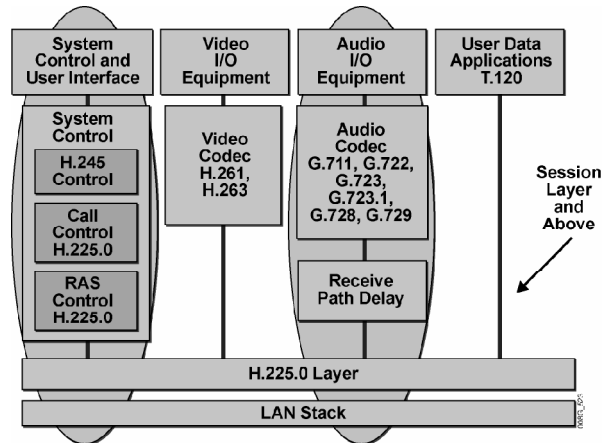
© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-1-3

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) has written the recommendation *H.323 Packet-based multimedia communications systems* (H.323). This recommendation describes an infrastructure of terminals, common control components, services, and protocols that are used for multimedia (voice, video, and data) communications.

An H.323 gateway is an optional type of endpoint that provides interoperability between H.323 endpoints and endpoints located on a switched-circuit network (SCN), such as the public switched telephone network (PSTN) or an enterprise voice network. Ideally, the gateway is transparent to both the H.323 endpoint and the SCN-based endpoint.

H.323 and Associated Recommendations

Cisco.com



The figure illustrates the elements of an H.323 terminal and highlights the protocol infrastructure of an H.323 endpoint.

H.323 originally was created to provide a mechanism for transporting multimedia applications over LANs. Although numerous vendors still use H.323 for videoconferencing applications, it has rapidly evolved to address the growing needs of VoIP networks. H.323 is currently the most widely used VoIP signaling and call control protocol, with international and domestic carriers relying on it to handle billions of minutes of use each year.

H.323 is considered an “umbrella protocol” because it defines all aspects of call transmission, including call establishment, capabilities exchange, and network resource availability. H.323 defines the following protocols:

- H.245 for capabilities exchange
- H.225.0 for call setup
- H.225.0 for Registration, Admission, and Status (RAS) control for call routing

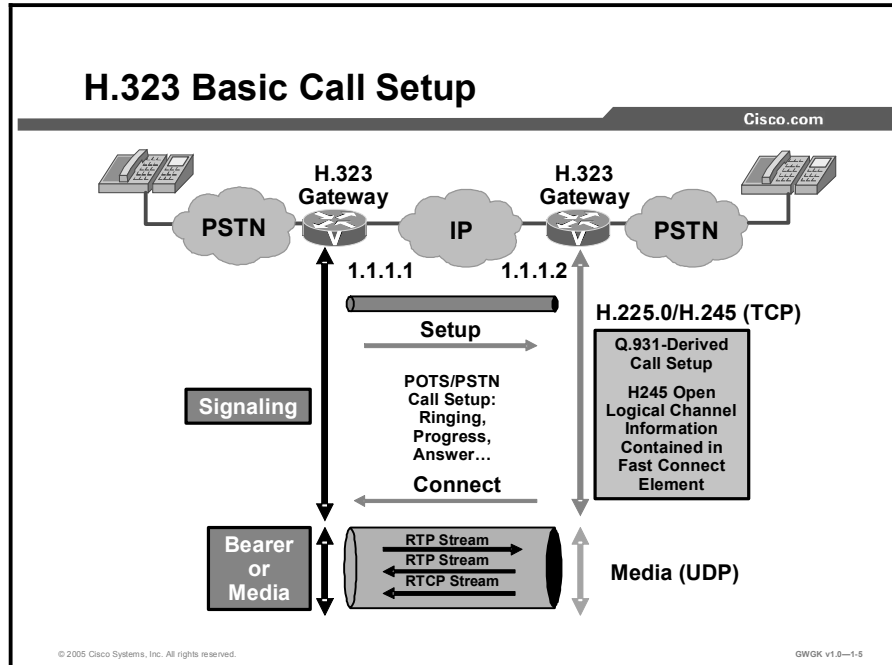
H.323 is based on the Integrated Services Digital Network (ISDN) Q.931 protocol, which allows H.323 to easily interoperate with traditional voice networks, such as the PSTN or Signaling System 7 (SS7). In addition to providing support for call setup, H.225.0 provides a message transport mechanism for the H.245 control function and the RAS signaling function. These functions are described as follows:

- **Call-signaling function:** This function uses a call-signaling channel that allows an endpoint to create connections with other endpoints. The call-signaling function defines call setup procedures, based on the call setup procedures for ISDN (Recommendation Q.931). The call-signaling function uses messages formatted according to H.225.0.

- **H.245 control function:** This function uses a control channel to transport control messages between endpoints or between an endpoint and a common control component, such as a gatekeeper or multipoint controller (MC). The control channel used by the H.245 control function is separate from the call-signaling channel. The H.245 control function is responsible for the following:
 - **Logical channel signaling:** Opens and closes the channel that carries the media stream
 - **Capabilities exchange:** Negotiates audio, video, and codec capability between the endpoints
 - **Master or responder determination:** Determines which endpoint is master and which is responder and is used to resolve conflicts during the call
 - **Mode request:** Requests a change in mode, or capability, of the media stream
 - **Timer and counter values:** Establishes values for timers and counters and agreement of those values by the endpoints
- **RAS signaling function:** This function uses a separate signaling channel (RAS channel) to perform registration, admissions and status procedures, bandwidth changes, and disengage procedures between endpoints and a gatekeeper. The RAS signaling function uses messages formatted according to H.225.0.

H.323 Call Flow

This topic describes a VoIP call flow entering and leaving a gateway and specifies how the call legs relate to dial peers.



The figure shows a H.323 setup exchange that uses the Fast Connect abbreviated procedure that is available in version 2 of Recommendation H.323. The Fast Connect procedure reduces the number of round-trip exchanges and achieves the capability exchange and logical channel assignments in one round trip.

The Fast Connect procedure includes these steps:

- Step 1** The originating gateway initiates an H.225.0 session with the destination gateway on registered TCP port 1720.
- Step 2** Call setup procedures based on Q.931 create a combined call-signaling channel and control channel for H.245. Capabilities and logical channel descriptions are exchanged within the Q.931 call setup procedure.
- Step 3** The logical channel descriptions are sent to open RTP sessions.
- Step 4** The endpoints exchange multimedia over the RTP sessions.

Note Cisco H.323 voice equipment supports up to version 4 of H.323 and is backward compatible to earlier versions.

Overview of MGCP Gateways

This topic describes the functions performed by a typical Media Gateway Control Protocol (MGCP) gateway.

Overview of MGCP Gateways

Cisco.com

- Call processing is done by a call agent such as Cisco CallManager.
- MGCP gateways handle the translation between audio signals and the packet network.
- Configuration commands for MGCP define this information:
 - The path between the call agent and the gateway
 - The type of gateway
 - The type of calls handled by the gateway
- MGCP uses endpoints and connections to construct a call.
 - Endpoints:
 - Sources of or destinations for data
 - Can be physical or logical locations in a device
 - Connections:
 - Point-to-point
 - Multipoint
- MGCP uses UDP for establishing audio connections over IP networks.

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-1-6

While H.323 enables gateways to process calls, MGCP, as defined under RFC 2705 and RFC 3435, takes all the signal and call processing out of the gateway and moves it to a call agent. The purpose of the gateway is to translate between audio signals and the packet network.

MGCP is an extension of the Simple Gateway Control Protocol (SGCP) and continues to support the SGCP. Systems using SGCP can easily migrate to MGCP. MGCP is a plain text protocol that uses a master-to-slave relationship between the call agent and the gateway to fully control the gateway and its associated ports. The plain-text commands are sent to gateways from the call agent using UDP port 2427. Port 2727 is used to send messages from the gateways to the call agent.

With MGCP, route patterns are configured on the Cisco CallManager, not by dial peers on the gateway. The gateway voice ports must be configured for proper signaling. However, there are no dial-peers for MGCP except when a router is using Cisco Survivable Remote Site Telephony (SRST) for fallback.

Configuration commands for MGCP define the path between the call agent and the gateway, the type of gateway, and the type of calls handled by the gateway. MGCP assumes a connection model where the basic constructs are endpoints and connections. Endpoints are sources or destinations of data or both and can be physical or virtual. Examples of physical and virtual endpoints are:

- An interface on a gateway that terminates a trunk connected to a Class 5 or Class 4 PSTN switch. A gateway that terminates trunks is called a trunking gateway.
- An interface on a gateway that terminates an analog plain old telephone service (POTS) connection to a phone, key system or PBX. A gateway that terminates residential POTS lines is called a residential gateway.

- An example of a virtual endpoint is an audio source in an audio-content server. Creation of physical endpoints requires hardware installation, while creation of virtual endpoints can be done by software.

Connections can be point-to-point or multipoint. A point-to-point connection is an association between two endpoints with the purpose of transmitting data between these endpoints. Once this association is established for both endpoints, data transfer between these endpoints can take place. A multipoint connection is established by connecting the endpoint to a multipoint session. Connections can be established over several types of bearer networks, such as:

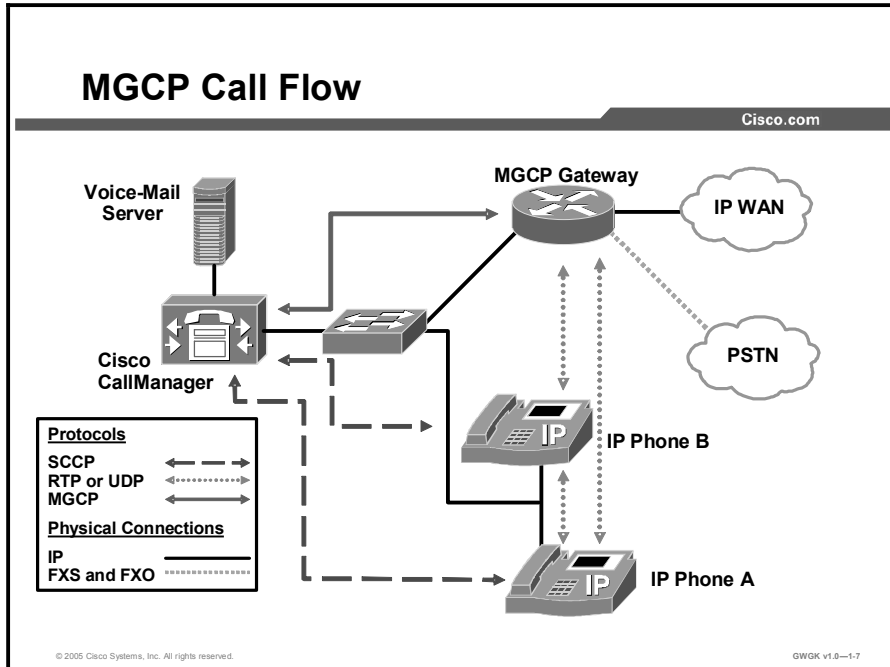
- Transmission of audio packets using Real-Time Transport Protocol (RTP) and User Datagram Protocol (UDP) over an IP network.
- Transmission of audio packets using Asynchronous Transfer Mode (ATM) adaptation layer 2 (AAL2), or another adaptation layer, over an ATM network.
- Transmission of packets over an internal connection, such as the time-division multiplexing (TDM) backplane or the interconnection bus of a gateway. This method is used, in particular, for “hairpin” connections that are connections that terminate in a gateway but are immediately rerouted over the telephone network.

Note For point-to-point connections, the endpoints of a connection could be in separate gateways or in the same gateway.

Similar to SGCP, MGCP uses UDP for establishing audio connections over IP networks. However, MGCP also uses hairpinning to return a call to the PSTN when the packet network is not available. Creating a call connection involves a series of signals and events that describe the connection process. This information might include such indicators as the off-hook event that triggers a dial-tone signal. These events and signals are specific to the type of endpoint that is involved in the call. MGCP groups these events and signals into packages. A trunk package, for example, is a group of events and signals related to a trunking gateway, while an announcement package groups events and signals for an announcement server.

MGCP Call Flow

This topic describes a VoIP call flow through an MGCP gateway, and specifies how the call legs relate to dial peers.



The figure illustrates how MGCP is used for call control purposes only and shows how voice data transfer occurs directly between the phone and the gateway.

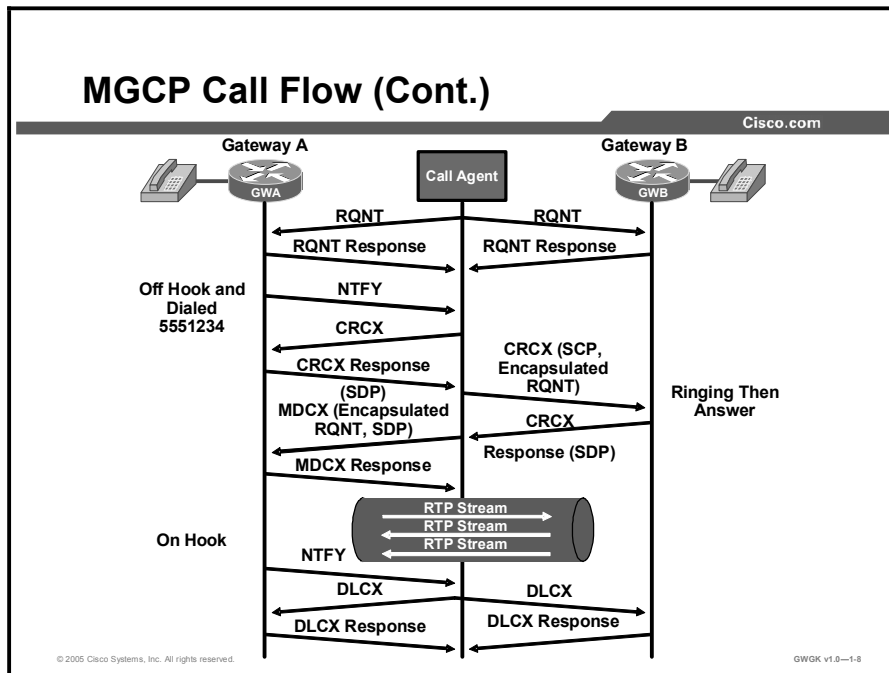
The Cisco 7960 IP Phones in this example use the Skinny Call Control Protocol (SCCP) to communicate with the Cisco CallManager. The actual voice data is transferred through RTP directly between the two devices. MGCP is used by the Cisco CallManager only to control the gateway.

MGCP service consists of nine connection and endpoint handling commands. These services allow a controller, which is normally the call agent, to instruct a gateway on the creation of connections that terminate in an endpoint attached to the gateway, and to be informed about events occurring at the endpoint. The “MGCP Control Commands” table provides an explanation of these commands.

MGCP Control Commands

Command	Purpose	Issued By
EndpointConfiguration	The call agent can issue an endpoint configuration (EPCF) command to a gateway, to instruct the gateway about the coding characteristics expected by the line-side of the endpoint.	Call agent
NotificationRequest	The call agent can issue a notification request (RQNT) command to a gateway to instruct the gateway to watch for specific events such as hook actions or DTMF tones on a specified endpoint.	Call agent
Notify	The gateway then uses the notify (NTFY) command to inform the call agent when the requested events occur.	Call agent
CreateConnection	The call agent can use the create connection (CRCX) command to create a connection that terminates in an endpoint inside the gateway.	Gateway
ModifyConnection	The call agent can use the modify connection (MDCX) command to change the parameters associated with a previously established connection.	Call agent
DeleteConnection	The call agent can use the delete connection (DLCX) command to delete an existing connection. The DLCX command may also be used by a gateway to indicate that a connection can no longer be sustained.	Call agent
AuditEndpoint	The call agent can use the audit endpoint (AUPE) and audit connection (AUCX) commands to audit the status of an endpoint and any connections associated with it. Network management beyond the capabilities provided by these commands is desirable. Such capabilities are to be supported by the use of the Simple Network Management Protocol (SNMP) and definition of a Management Information Base (MIB) which is outside the scope of this discussion.	Call agent
AuditConnection	(See the description for the AUPE command.)	Call agent or gateway
RestartInProgress	The gateway can use the ReStart In Progress (RSIP) command to notify the call agent that a group of endpoints managed by the gateway is being taken out of service or is being placed back in service.	Call agent

MGCP Call Flow (Cont.)



The figure illustrates a dialog between a call agent and two gateways. Although the gateways in this example are both residential gateways, the “MGCP Call Flow” table presents principles of operation. These are the same for other gateway types.

MGCP Call Flow

Step	Action	Notes
1.	The call agent sends an RQNT message to each gateway.	Because they are residential gateways, the request instructs the gateways to wait for an off-hook transition (event). When the off-hook transition event occurs, the call agent instructs the gateways to supply a dial tone (signal). The call agent asks the gateway to monitor for other events as well. By providing a digit map in the request, the call agent can have the gateway collect digits before it notifies the call agent.
2.	The gateways respond (shown as RQNT Response in the figure) to the request.	At this point, the gateways and the call agent wait for a triggering event.
3.	A user on Gateway A goes off hook.	As instructed by the call agent in its earlier request, the gateway provides a dial tone. Because the gateway is provided with a digit map, it begins to collect digits (as they are dialed) until either a match is made or no match is possible. For the remainder of this example, assume that the digits match a digit map entry.
4.	Gateway A sends the NTFY message to the call agent to advise the call agent that a requested event was observed.	The NTFY identifies the endpoint, the event, and, in this case, the dialed digits.

Step	Action	Notes
5.	After confirming that a call is possible based on the dialed digits, the call agent instructs Gateway A to create a connection with its endpoint (via the CRCX message).	
6.	The gateway sends a CRCX message with a Session Description Protocol (SDP) if it is able to accommodate the connection.	The session description identifies at least the IP address and UDP port for use in a subsequent RTP session. The gateway does not have a session description for the remote side of the call, and the connection enters a wait state.
7.	The call agent prepares and sends a connection request (shown as "CRCX, SDP Encapsulated RQNT" in the figure) to Gateway B.	In the request, the call agent provides the session description obtained from Gateway A. The connection request is targeted to a single endpoint—if only one endpoint is capable of handling the call—or to any one of a set of endpoints. The call agent also embeds a notification request that instructs the gateway about the signals and events that it should now consider relevant. In this example, in which the gateway is residential, the signal requests ringing and the event is an off-hook transition. Note: The interaction between Gateway B and its attached user has been simplified.
8.	Gateway B responds to the request with its session description (shown as "CRCX Response, SDP" in the figure).	Notice that Gateway B has both session descriptions and recognizes how to establish its RTP sessions.
9.	The call agent relays the session description to Gateway A in an MDCX request.	This request may contain an encapsulated notify request that describes the relevant signals and events at this stage of the call setup. Now Gateway A and Gateway B have the required session descriptions to establish the RTP sessions over which the audio travels.
10.	At the conclusion of the call, one of the endpoints recognizes an on-hook transition.	In the example, the user on Gateway A hangs up. Because the call agent requested the gateways to notify in such an event, Gateway A notifies the call agent.
11.	The call agent sends a DLCX request to each gateway.	
12.	The gateways delete the connections and responds to the call agent.	

Overview of SIP Gateways

This topic describes the functions performed by a typical SIP gateway.

Overview of SIP Gateways

Cisco.com

- **SIP was developed by the IETF for multimedia conferencing over IP.**
- **SIP also provides nonproprietary advantages in the following areas:**
 - **Protocol extensibility**
 - **System scalability**
 - **Personal mobility services**
 - **Interoperability with different vendors**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-1.9

Session Initiation Protocol (SIP) is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate multimedia sessions such as Internet telephony calls between two or more endpoints. SIP can also invite participants to existing sessions such as multicast conferences, and media can be added to and removed from an existing session. SIP transparently supports name mapping and redirection services, which supports personal mobility so users can maintain a single externally visible identifier regardless of their network location.

SIP was developed by the Internet Engineering Task Force (IETF). Its features are compliant with IETF RFC 2543, *SIP: Session Initiation Protocol*, published in March 1999 and IETF RFC 3261, *SIP: Session Initiation Protocol*, published in June 2002.

Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

The Cisco SIP functionality enables voice gateways to signal the setup of voice and multimedia calls over IP networks. The SIP feature also provides nonproprietary advantages in the following areas:

- Protocol extensibility
- System scalability
- Personal mobility services
- Interoperability with different vendors

SIP Capabilities

Cisco.com

SIP provides the following capabilities:

- **Determines the location of the target endpoint**
- **Determines the media capabilities of the target endpoint**
- **Determines the availability of the target endpoint**
- **Establishes a session between the originating and target endpoints**
- **Handles the transfer and termination of calls**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-10

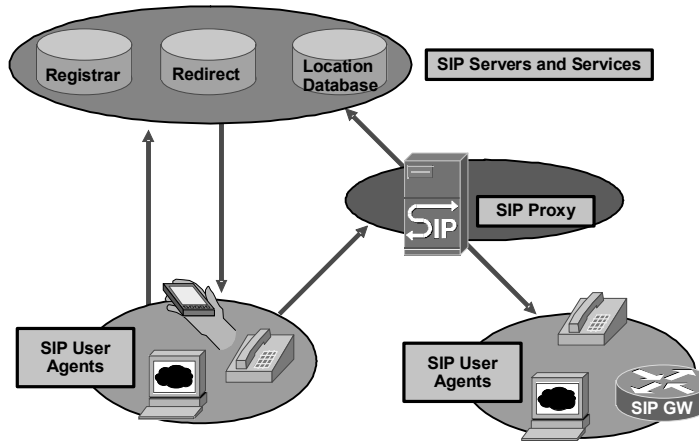
SIP provides the following capabilities:

- **Determines the location of the target endpoint:** SIP supports address resolution, name mapping, and call redirection.
- **Determines the media capabilities of the target endpoint:** SIP determines the lowest level of common services between the endpoints through Session Description Protocol (SDP). Conferences are established using only the media capabilities that can be supported by all endpoints.
- **Determines the availability of the target endpoint:** If a call cannot be completed because the target endpoint is unavailable, SIP determines whether the called party is connected to a call already or did not answer in the allotted number of rings. SIP then returns a message indicating why the target endpoint was unavailable.
- **Establishes a session between the originating and target endpoints:** If the call can be completed, SIP establishes a session between the endpoints. SIP also supports midcall changes, such as the addition of another endpoint to the conference or the changing of a media characteristic or codec.
- **Handles the transfer and termination of calls:** SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions among all parties.

Note The term “conference” describes an established session (or call) between two or more endpoints. Conferences consist of two or more users and can be established using multicast or multiple unicast sessions.

SIP Network Topology

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-11

SIP is modeled on the interworking of user agents and network servers. This section describes the functional and physical components of a user agent.

SIP is a peer-to-peer protocol. The peers in a session are called user agents. A user agent consists of two functional components:

- **User agent client (UAC):** A client application that initiates a SIP request.
- **User agent server (UAS):** A server application that contacts the user when a SIP invitation is received and then returns a response on behalf of the user to the invitation originator.

Typically, a SIP user agent can function as a UAC or a UAS during a session but not as both in the same session. Whether the endpoint functions as a UAC or a UAS depends on the user agent that initiated the request. The initiating user agent uses a UAC and the terminating user agent uses a UAS.

From an architectural standpoint, the physical components of a SIP network are grouped as follows:

- **User agents:** SIP user agents include the following devices:
 - **IP phone:** Acts as a UAS or UAC on a session-by-session basis. Software telephones and Cisco SIP IP phones initiate SIP requests and respond to requests.
 - **Gateway:** Acts as a UAS or UAC and provides call control support. Gateways provide many services, and the most common is a translation function between SIP user agents and other terminal types. This function includes translation between transmission formats and between communications procedures. A gateway translates between audio and video signals and performs call setup and clearing on both the IP side and the switched-circuit network (SCN) side.

- **SIP servers:** SIP servers include the following types:
 - **Proxy server:** An intermediate component that receives SIP requests from a client, then forwards the requests on behalf of the client to the next SIP server in the network. The next server can be another proxy server or a UAS. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request transmissions, and security.
 - **Redirect server:** Provides a user agent with information about the next server that the user agent should contact. The server can be another network server or a user agent. The user agent redirects the invitation to the server identified by the redirect server.
 - **Registrar server:** Responds to requests from UACs for registration of their current location. Registrar servers are often located near or with other network servers, most often a location server.
 - **Location server:** An abstraction of a service providing address resolution services to SIP proxy or redirect servers. A location server embodies mechanisms to resolve addresses. These mechanisms can include a database of registrations or access to commonly used resolution tools such as finger, rwhois, Lightweight Directory Access Protocol (LDAP), or operating system-dependent mechanisms. A registrar server can be modeled as one subcomponent of a location server. The registrar server is partly responsible for populating a database associated with the location server.

Note Except for the REGISTER mode request, communication between SIP components and a location server is not standardized.

SIP Call Flow

This topic describes a VoIP call flow entering and leaving a SIP gateway, highlighting the call legs relative to dial peers.

SIP Methods

Cisco.com

- **All SIP messages are either requests from a server or client or responses to a request.**
- **SIP uses six basic types (methods) of requests:**
 - **INVITE**—Indicates a user or service is being invited to participate in a call session
 - **ACK**—Confirms client has final response to an INVITE request
 - **BYE**—Terminates a call
 - **CANCEL**—Cancels pending searches, does not terminate a call that has already been accepted
 - **OPTIONS**—Queries the capabilities of servers
 - **REGISTER**—Registers the address listed in the to header field with a SIP server

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0—1-12

All SIP messages, referred to as “methods,” are either requests from a server or client or responses to a request. The messages are formatted according to RFC 822, *Standard for the format of ARPA internet text messages*. For all messages, this is the general format:

- A start line
- One or more header fields
- An empty line
- A message body (optional)
 - Each line must end with a carriage return-line feed (CRLF).
- Requests: SIP uses six basic types (methods) of requests:
 - **INVITE:** Indicates a user or service is being invited to participate in a call session. The gateway supports mid-call INVITEs with the same call ID but different SDP session parameters (to change the transport address). An invitation occurs when one SIP endpoint (User A) invites another SIP endpoint (User B) to join in a call. During this process, User A sends an INVITE message requesting that User B join a particular conference or establish a two-party conversation. If User B wants to join the call, it sends an affirmative response (SIP 2xx). Otherwise, it sends a failure response (SIP 4xx). After receiving the response, User A acknowledges the response with an ACK message. If User A no longer wants to establish this conference, it sends a BYE message instead of an ACK message.
 - **ACK:** Confirms that the client has received a final response to an INVITE request.
 - **BYE:** Terminates a call and can be sent by either the caller or the called party.

- **CANCEL:** Cancels any pending searches but does not terminate a call that has already been accepted.
- **OPTIONS:** Queries the capabilities of servers. The gateway does not generate OPTIONS. However, it will respond to OPTIONS requests.
- **REGISTER:** Registers the address listed in the To header field with a SIP server. A registration occurs when a client needs to inform a proxy or redirect server of its location. During this process, the client sends a REGISTER request to the proxy or redirect server and includes the address (or addresses) at which it can be reached.
- Other methods the gateways can respond to:
 - **COnditions MET (COMET):** Used in QoS implementation to indicate to other endpoints whether or not the conditions have been met (for example, resources reserved).
 - **NOTIFY:** Used in implementations of REFER to let the initiator of the REFER message know the outcome of the transfer.
 - **PRovisional ACKnowledgement (PRACK):** Used in reliable provisional responses.
 - **REFER:** Gateways respond to a REFER, but they do not generate a REFER for transfer.
 - **SUBSCRIBE:** Gateways process SUBSCRIBE for telephony events such as DTMF and for Message Waiting Indication (MWI).
 - **INFO:** Gateways do not generate INFO methods. Gateways can handle incoming INFO methods.

SIP Responses

Cisco.com

- **1xx Response—Information responses**
- **2xx Response—Successful responses**
- **3xx Response—Redirection responses**
- **4xx Response—Request failure responses**
- **5xx Response—Server failure responses**
- **6xx Response—Global responses**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-14

The six SIP information responses and details are found in the “SIP Information Responses” table.

SIP Information Responses

SIP Response Type	Response Comment	Description
1xx Response—Information responses		
	100 Trying	This response indicates that action is being taken on behalf of the caller, but that the called party has not yet been located. The SIP gateway generates this response for an incoming INVITE. After receiving this response, the gateway stops retransmitting INVITEs. It then waits for a 180 Ringing or 200 OK response.
	180 Ringing	This response indicates that the called party has been located and is being notified of the call. The SIP gateway generates a 180 Ringing response when the called party has been located and is being alerted. After receiving this response, the gateway waits for a 200 OK response.
	181 Call is being forwarded	This response indicates that the call is being rerouted to another destination. The SIP gateway does not generate this response. After receiving this response, the gateway processes the responses the same way that it processes a 100 Trying response.
	182 Queued	This response indicates that the called party is not currently available but that they have elected to queue the call rather than reject it.
	183 Session progress	This response is used to perform in-band alerting for the caller. The SIP gateway generates a 183 Session progress response when it receives an ISDN Progress message with an appropriate media indication from the PSTN.

SIP Response Type	Response Comment	Description
2xx Response—Successful responses		
	200 OK	This response indicates that the request has been successfully processed. The action taken depends on the request made. The SIP gateway generates this response when the PBX indicates that the user has answered the phone. After receiving this response, the gateway forwards the response to the corresponding party and responds with an ACK.
3xx Response—redirection		
	300 Multiple Choices	This response indicates that the address resolved to more than one location. All locations are provided and the user or user agent is allowed to select which location to use. The SIP gateway does not generate this response. After receiving this response, the gateway contacts the new address in the Contact header field.
	301 Moved Permanently	This response indicates that the user is no longer available at the specified location. An alternate location is included in the header.
	302 Moved Temporarily	This response indicates that the user is temporarily unavailable at the specified location. An alternate location is included in the header.
	305 Use Proxy	This response indicates that the caller must use a proxy to contact the called party.
	380 Alternative Service	This response indicates that the call was unsuccessful, but that alternative services are available.
4xx Response—Request failure responses		
	400 Bad Request	This response indicates that the request could not be understood because of an illegal format. The SIP gateway generates a 400 Bad Request response for a badly formed request. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	401 Unauthorized	This response indicates that the request requires user authentication. The SIP gateway does not generate this response. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	402 Payment Required	This response indicates that payment is required to complete the call.
	403 Forbidden	This response indicates that the server has received and understood the request but will not provide the service.
	404 Not Found	This response indicates that the server has definite information that the user does not exist in the specified domain. The SIP gateway generates this response if it is unable to locate the called party. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.

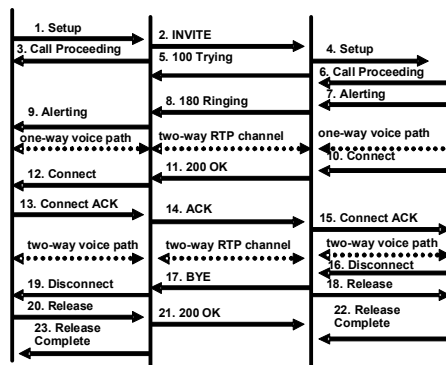
SIP Response Type	Response Comment	Description
	405 Method Not Allowed	This response indicates that the method specified in the request is not allowed. The response contains a list of allowed methods. The SIP gateway generates this response if an invalid method is specified in the request. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	406 Not Acceptable	This response indicates that the requested resource is capable of generating only responses that have content characteristics not acceptable as specified in the accept header of the request. The SIP gateway does not generate this response. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	407 Proxy authentication required	This response is similar to the 401 Unauthorized response. However, this response indicates that the client must first authenticate itself with the proxy. The SIP gateway does not generate this response. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	408 Request timeout	This response indicates that the server could not produce a response before the Expires messages time out.
	409 Conflict	This response indicates that the request could not be processed because of a conflict with the current state of the resource.
	410 Gone	This response indicates that a resource is no longer available at the server and no forwarding address is known. The SIP gateway generates this response if the PSTN returns a cause code of unallocated number. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	411 Length Required	This response indicates that the user refuses to accept the request without a defined content length. The SIP gateway does not generate this response. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	413 Request Entity Too Large	This response indicates that server refuses to process the request because it is larger than the server is willing or able to process.
	414 Request-URI Too Long	This response indicates that the server refuses to process the request because the Request-uniform resource identifier (URI) is too long for the server to interpret.
	415 Unsupported Media	This response indicates that the server refuses to process the request because the format of the body is not supported by the destination endpoint.
	420 Bad Extension	This response indicates that the server could not understand the protocol extension indicated in the Require header. The SIP gateway generates this response if it cannot understand the service requested in the Require header field. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.

SIP Response Type	Response Comment	Description
	480 Temporarily Unavailable	This response indicates that the called party was contacted but is temporarily unavailable. The SIP gateway generates this response if the called party is unavailable (for example, the called party does not answer the phone within a certain amount of time or the called number does not exist or is no longer in service). After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	481 Call Leg/Transaction Does not Exist	This response indicates that the server is ignoring the request because it was either a BYE for which there was no matching leg ID or a CANCEL for which there was no matching transaction. The SIP gateway generates this response if the call leg ID or transaction cannot be identified. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	482 Loop Detected	This response indicates that the server received a request that included itself in the path. The SIP gateway does not generate this response. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	483 Too Many Hops	This response indicates that the server received a request that required more hops than allowed by the Max-Forwards header.
	484 Address Incomplete	This response indicates that the server received a request containing an incomplete address.
	485 Ambiguous	This response indicates that the server received a request in which the called party address was ambiguous. It can provide possible alternate addresses.
	486 Busy Here	This response indicates that the called party was contacted but that their system is unable to take additional calls. The SIP gateway generates this response if the called party was contacted but was busy. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	487 Request Cancelled	This response indicates that the request was terminated by a BYE or CANCEL request. The SIP gateway generates this response to an unexpected BYE or CANCEL received for a request.
	488 Not Acceptable Media	This response indicates an error in handling the request at this time. The SIP gateway generates this response if the media negotiation fails.
	422 Session Timer Too Small	It is generated by the gateway (UAS) when a request contains a Session-Expires header with a duration that is below the minimum timer for the gateway server. The 422 response MUST contain a Min-SE header with a minimum timer for that server.
5xx Response— Server failure responses		
	500 Server Internal Error	This response indicates that the server or gateway encountered an unexpected error that prevented it from processing the request. The SIP gateway generates this response if it encountered an unexpected error that prevented it from processing the request. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.

SIP Response Type	Response Comment	Description
	501 Not Implemented	This response indicates that the server or gateway does not support the functions required to complete the request.
	502 Bad Gateway	This response indicates that the server or gateway received an invalid response from a downstream server.
	503 Service Unavailable	This response indicates that the server or gateway is unable to process the request due to an overload or maintenance problem.
	504 Gateway timeout	This response indicates that the server or gateway did not receive a timely response from another server (such as a location server).
	505 Version Not supported	This response indicates that the server or gateway does not support the version of the SIP protocol used in the request.
	580 Precondition failed	The SIP gateway uses this response code to indicate a failure in having QoS preconditions met for a call.
6xx Response— Global responses		
	600 Busy Everywhere	This response indicates that the called party was contacted but that the called party is busy and cannot take the call at this time. The SIP gateway does not generate this response. After receiving this response, the gateway initiates a graceful call disconnect and clears the call.
	603 Decline	This response indicates that the called party was contacted but cannot or does not want to participate in the call.
	604 Does Not Exist Anywhere	This response indicates that the server has authoritative information that the called party does not exist in the network.
	606 Not Acceptable	This response indicates that the called party was contacted, but that some aspect of the session description was unacceptable.

SIP Gateway-to-SIP Gateway: Call Flow Setup and Disconnect

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-15

SIP is based on an HTTP-like request-response transaction model. Each transaction consists of a request that invokes a particular method, or function, on the server and at least one response. The figure illustrates a successful gateway-to-gateway call setup and disconnect.

The two end users are User A and User B. User A is located at PBX A, which is connected to SIP Gateway 1 via a T1 or E1. User B is located at PBX B, which is connected to SIP Gateway 2 via a T1 or E1. The User B phone number is 555-0100. SIP Gateway 1 is connected to SIP Gateway 2 over an IP network. The call flow scenario is as follows:

1. User A calls User B
2. User B answers the call
3. User B hangs up

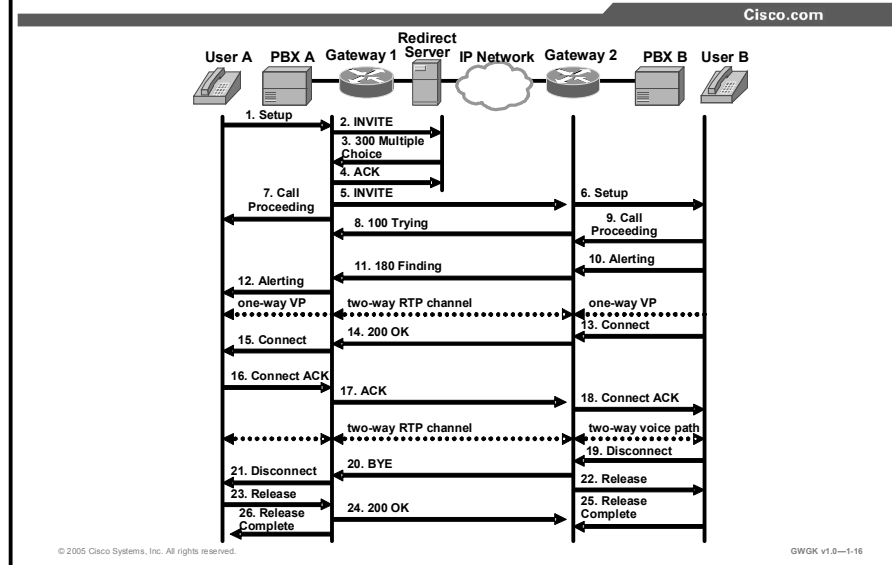
SIP Gateway-to-SIP Gateway Call Flow Setup and Disconnect

Step	Action	Description
1.	Setup—PBX A to SIP Gateway 1	Call setup is initiated between PBX A and SIP Gateway 1. Setup includes the standard transactions that take place as User A attempts to call User B.
2.	INVITE—SIP Gateway 1 to SIP Gateway 2	<p>SIP Gateway 1 sends an INVITE request to SIP Gateway 2. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request the following is the case:</p> <ul style="list-style-type: none"> ■ The phone number of User B is inserted in the Request-URI field in the form of an SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as “INVITE sip:555-0100@companyb.com; user=phone.” The “user=phone” parameter indicates that the Request-URI address is a telephone number rather than a user name. ■ PBX A is identified as the call session initiator in the From field. ■ A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ■ The transaction number within a single call leg is identified in the CSeq field. ■ The media capability User A is ready to receive is specified. ■ The port on which SIP Gateway 1 is prepared to receive the RTP data is specified.
3.	Call Proceeding—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Call Proceeding message to PBX A to acknowledge the setup request.
4.	Setup—SIP Gateway 2 to PBX B	SIP Gateway 2 receives the INVITE request from SIP Gateway 1 and initiates call setup with User B via PBX B
5.	100 Trying—SIP Gateway 2 to SIP Gateway 1	SIP Gateway 2 sends a 100 Trying response to the INVITE request sent by SIP Gateway 1. The 100 Trying response indicates that the INVITE request has been received by SIP Gateway 2 but that User B has not yet been located and that some unspecified action, such as a database consultation, is taking place.
6.	Call Proceeding—PBX B to SIP Gateway 2	PBX B sends a Call Proceeding message to SIP Gateway 2 to acknowledge the setup request.
7.	Alerting—PBX B to SIP Gateway 2	PBX B locates User B and sends an Alert message to SIP Gateway 2. The User B phone rings.
8.	180 Ringing—SIP Gateway 2 to SIP Gateway 1	SIP Gateway 2 sends a 180 Ringing response to SIP Gateway 1. The 180 Ringing response indicates that SIP Gateway 2 has located, and is trying to alert, User B.
9.	Alerting—SIP Gateway 1 to PBX A	A SIP Gateway 1 sends an Alert message to User A via PBX A. The Alert message indicates that SIP Gateway 1 has received a 180 Ringing response from SIP Gateway 2. User A hears the ringback tone that indicates that User B is being alerted. At this point, a one-way voice path is established between SIP Gateway 1 and PBX A and between SIP Gateway 2 and PBX B. A two-way RTP channel is established between SIP Gateway 1 and SIP Gateway 2.

Step	Action	Description
10.	Connect—PBX B to SIP Gateway 2	User B answers phone. PBX B sends a Connect message to SIP Gateway 2. The Connect message notifies SIP Gateway 2 that the connection has been made.
11.	200 OK—SIP Gateway 2 to SIP Gateway 1	SIP Gateway 2 sends a 200 OK response to SIP Gateway 1. The 200 OK response notifies SIP Gateway 1 that the connection has been made. If User B supports the media capability advertised in the INVITE message sent by SIP Gateway 1, it advertises the intersection of its own and User A media capability in the 200 OK response. If User B does not support the media capability advertised by User A, it sends back a 400 Bad Request response with a 304 Warning header field.
12.	Connect—SIP Gateway 1 to PBX A	A SIP Gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
13.	Connect ACK—PBX A to SIP Gateway 1	PBX A acknowledges the Connect message from SIP Gateway 1.
14.	ACK—SIP Gateway 1 to SIP Gateway 2	SIP Gateway 1 sends an ACK to SIP Gateway 2. The ACK confirms that SIP Gateway 1 has received the 200 OK response from SIP Gateway 2.
15.	Connect ACK—SIP Gateway 2 to PBX B	SIP Gateway 2 acknowledges the Connect message from PBX B. The call session is now active over a two-way voice path via Real-time Transport Protocol (RTP). At this point, a two-way voice path is established between SIP Gateway 1 and PBX A and between SIP Gateway 2 and PBX B. A two-way RTP channel is established between SIP Gateway 1 and SIP Gateway 2.
16.	Disconnect—PBX B to SIP Gateway 2	Once User B hangs up, PBX B sends a Disconnect message to SIP Gateway 2. The Disconnect message starts the call session termination process.
17.	BYE—SIP Gateway 2 to SIP Gateway 1	SIP Gateway 2 sends a BYE request to SIP Gateway 1. The BYE request indicates that User B wants to release the call. Because User B is the one that wants to terminate the call, the Request-URI field is now replaced with the SIP URL of PBX A, and the From field contains the SIP URL of User B. The CSeq value is incremented by one. Note: RFC 3261 requires that a UAS that receives a BYE request first send a response to any pending requests for that call before disconnecting. After receiving a BYE request, the UAS should respond with a 487 (Request Cancelled) status message.
18.	Release—SIP Gateway 2 to PBX B	SIP Gateway 2 sends a Release message to PBX B.
19.	Disconnect—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Disconnect message to PBX A.
20.	Release—PBX A to SIP Gateway 1	PBX A sends a Disconnect message to SIP Gateway 1.
21.	200 OK—SIP Gateway 1 to SIP Gateway 2	SIP Gateway 1 sends a 200 OK response to SIP Gateway 2. The 200 OK response notifies SIP Gateway 2 that SIP Gateway 1 has received the BYE request.
22.	Release Complete—PBX B to SIP Gateway 2	PBX B sends a Release Complete message to SIP Gateway 2.

Step	Action	Description
23.	Release Complete—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Release Complete message to PBX A and the session is terminated.

SIP Gateway-to-SIP Gateway Call Flow via SIP Redirect Server



The figure illustrates a successful gateway-to-gateway call setup and disconnect via a SIP redirect server. In this scenario, the two end users are identified as User A and User B. User A is located at PBX A. PBX A is connected to SIP Gateway 1 via a T1 or E1. SIP Gateway 1 is using a SIP redirect server. User B is located at PBX B. PBX B is connected to SIP Gateway 2 via a T1 or E1. The User B phone number is 555-0002. SIP Gateway 1 is connected to SIP Gateway 2 over an IP network.

The call flow scenario is as follows:

1. User A calls User B via SIP Gateway 1 using a SIP redirect server.
2. User B answers the call.
3. User B hangs up.

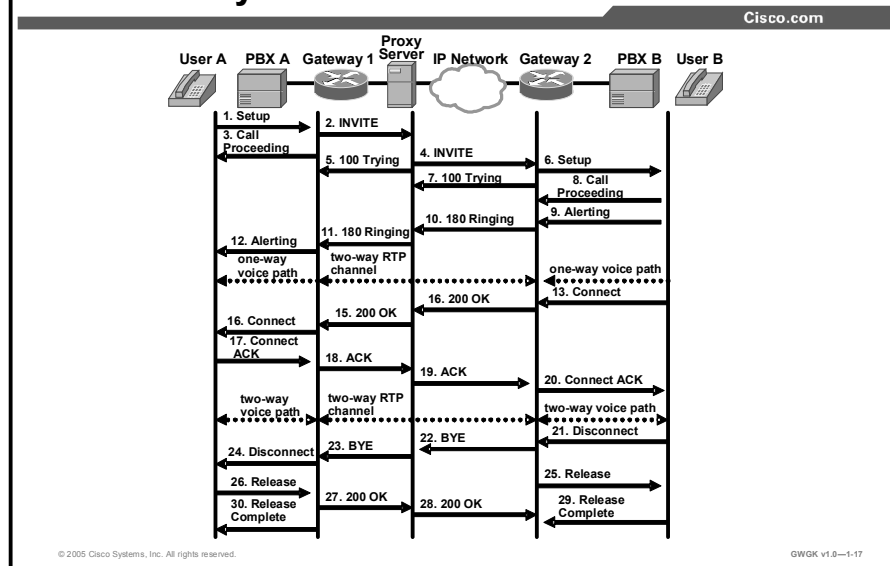
SIP Gateway-to-SIP Gateway Call Flow via SIP Redirect Server

Step	Action	Description
1.	Setup—PBX A to SIP Gateway 1	Call Setup is initiated between PBX A and SIP Gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2.	INVITE—SIP Gateway 1 to SIP Redirect Server	<p>SIP Gateway 1 sends an INVITE request to the SIP redirect server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> ■ Insert the phone number of User B in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter distinguishes that the Request-URI address is a telephone number rather than a user name. ■ PBX A is identified as the call session initiator in the From field. ■ A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ■ The transaction number within a single call leg is identified in the CSeq field. ■ The media capability User A is ready to receive is specified. ■ The port on which SIP Gateway 1 is prepared to receive the RTP data is specified.
3.	300 Multiple Choice—SIP Redirect Server to SIP Gateway 1	<p>The SIP redirect server sends a 300 Multiple Choice response to SIP Gateway 1.</p> <p>The 300 Multiple Choice response indicates that the SIP redirect server accepted the INVITE request, contacted a location server with all or part of the User B SIP URL, and the location server provided a list of alternative locations where User B might be located. The SIP redirect server returns these possible addresses to SIP Gateway 1 in the 300 Multiple Choice response.</p>
4.	ACK—SIP Gateway 1 to SIP Redirect Server	SIP Gateway 1 acknowledges the 300 Multiple Choice response with an ACK.
5.	INVITE—SIP Gateway 1 to SIP Gateway 2	SIP Gateway 1 sends a new INVITE request to SIP Gateway 2. The new INVITE request includes the first contact listed in the 300 Multiple Choice response as the new address for User B, a higher transaction number in the CSeq field, and the same Call-ID as the first INVITE request.
6.	Setup—SIP Gateway 2 to PBXB	SIP Gateway 2 receives the INVITE request from SIP Gateway 1 and initiates a Call Setup with User B via PBXB.
7.	Call Proceeding—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.

Step	Action	Description
8.	100 Trying—SIP Gateway 2 to SIP Gateway 1	SIP Gateway 2 sends a 100 Trying response to the INVITE request sent by SIP Gateway 1. The 100 Trying response indicates that the INVITE request has been received by SIP Gateway 2 but that User B has not yet been located.
9.	Call Proceeding—PBX B to SIP Gateway 2	PBX B sends a Call Proceeding message to SIP Gateway 2 to acknowledge the Call Setup request.
10.	Alerting—PBX B to SIP Gateway 2	PBX B locates User B and sends an Alert message to SIP Gateway 2. The User B phone begins to ring.
11.	180 Ringing—SIP Gateway 2 to SIP Gateway 1	SIP Gateway 2 sends a 180 Ringing response to SIP Gateway 1. The 180 Ringing response indicates that SIP Gateway 2 has located, and is trying to alert, User B.
12.	Alerting—SIP Gateway 1 to PBX A	SIP Gateway 1 sends an Alert message to PBX A. User A hears ringback tone. At this point, a one-way voice path is established between SIP Gateway 1 and PBX A and between SIP Gateway 2 and PBX B. A two-way RTP channel is established between SIP Gateway 1 and SIP Gateway 2.
13.	Connect—PBX B to SIP Gateway 2	User B answers phone. PBX B sends a Connect message to SIP Gateway 2. The Connect message notifies SIP Gateway 2 that the connection has been made.
14.	200 OK—SIP Gateway 2 to SIP Gateway 1	SIP Gateway 2 sends a 200 OK response to SIP Gateway 1. The 200 OK response notifies SIP Gateway 1 that the connection has been made. If User B supports the media capability advertised in the INVITE message sent by SIP Gateway 1, it advertises the intersection of its own and User A media capability in the 200 OK response. If User B does not support the media capability advertised by User A, it sends back a 400 Bad Request response with a 304 Warning header field.
15.	Connect—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
16.	Connect ACK—PBX A to SIP Gateway 1	PBX A acknowledges the Connect message from SIP Gateway 1.
17.	ACK—SIP Gateway 1 to SIP Gateway 2	SIP Gateway 1 sends an ACK to SIP Gateway 2. The ACK confirms that the 200 OK response has been received. The call is now in progress over a two-way voice path via RTP.
18.	Connect ACK—SIP Gateway 2 to PBX B	SIP Gateway 2 acknowledges the Connect message from PBX B. At this point, a two-way voice path is established between SIP Gateway 1 and PBX A and between SIP Gateway 2 and PBX B. A two-way RTP channel is established between SIP Gateway 1 and SIP Gateway 2.
19.	Disconnect—PBX B to SIP Gateway 2	Once User B hangs up, PBX B sends a Disconnect message to SIP Gateway 2. The Disconnect message starts the call session termination process.

Step	Action	Description
20.	BYE—SIP Gateway 2 to SIP Gateway 1	SIP Gateway 2 sends a BYE request to SIP Gateway 1. The BYE request indicates that User B wants to release the call. Because it is User B that wants to terminate the call, the Request-URI field is now replaced with the SIP URL of PBX A and the From field contains the SIP URL of User B.
21.	Disconnect—SIP Gateway 1 to PBXA	SIP Gateway 1 sends a Disconnect message to PBX A.
22.	Release—SIP Gateway 2 to PBX B	SIP Gateway 2 sends a Release message to PBX B.
23.	Release—PBX A to SIP Gateway 1	PBX A sends a Release message to SIP Gateway 1.
24.	200 OK—SIP Gateway 1 to SIP Gateway 2	SIP Gateway 1 sends a 200 OK response to SIP Gateway 2. The 200 OK response notifies SIP Gateway 2 that SIP Gateway 1 has received the BYE request.
25.	Release Complete—PBX B to SIP Gateway 2	PBX B sends a Release Complete message to SIP Gateway 2.
26.	Release Complete—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Release Complete message to PBX A and the session is terminated.

SIP Gateway-to-SIP Gateway Call Flow via SIP Proxy Server



The figure illustrates a successful gateway-to-gateway call setup and disconnect via a proxy server. In this scenario, the two end users are User A and User B. User A is located at PBX A. PBX A is connected to SIP Gateway 1 via a T1 or E1. SIP Gateway 1 is using a proxy server. SIP Gateway 1 is connected to SIP Gateway 2 over an IP network. User B is located at PBX B. PBX B is connected to SIP Gateway 2 (a SIP gateway) via a T1 or E1. The User B phone number is 555-0002.

In the scenario, the record route feature is enabled on the proxy server. When record route is enabled, the proxy server adds the Record-Route header to the SIP messages to ensure that it is in the path of subsequent SIP requests for the same call leg. The Record-Route field contains a globally reachable Request-URI that identifies the proxy server. When record route is enabled, each proxy server adds its Request-URI to the beginning of the list.

When record route is disabled, SIP messages flow directly through the SIP gateways once a call has been established.

The call flow is as follows:

1. User A calls User B via SIP Gateway 1 using a proxy server.
2. User B answers the call.
3. User B hangs up.

SIP Gateway-to-SIP Gateway Call Flow via SIP Proxy Server

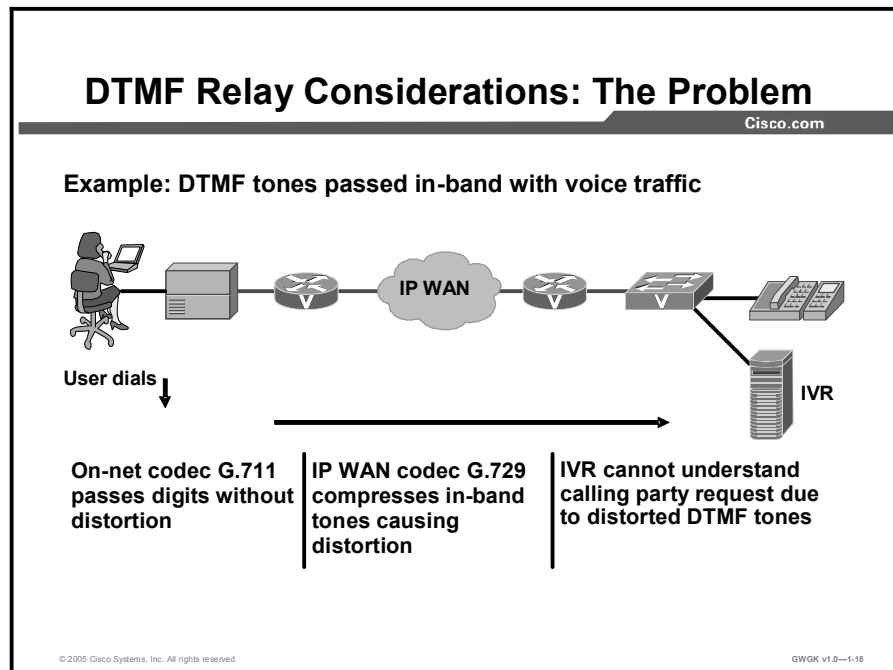
Step	Action	Notes
1.	Setup—PBX A to SIP Gateway 1	Call Setup is initiated between PBX A and SIP Gateway 1. The Call Setup includes the standard transactions that take place as User A attempts to call User B.
2.	2 INVITE—SIP Gateway 1 to Proxy Server	<p>SIP Gateway 1 sends an INVITE request to the SIP proxy server. The INVITE request is an invitation to User B to participate in a call session.</p> <p>In the INVITE request:</p> <ul style="list-style-type: none"> ■ Insert the phone number of User B in the Request-URI field in the form of a SIP URL. The SIP URL identifies the address of User B and takes a form similar to an email address (<i>user@host</i> where <i>user</i> is the telephone number and <i>host</i> is either a domain name or a numeric network address). For example, the Request-URI field in the INVITE request to User B appears as "INVITE sip:555-0002@companyb.com; user=phone." The "user=phone" parameter distinguishes that the Request-URI address is a telephone number rather than a user name. ■ PBX A is identified as the call session initiator in the From field. ■ A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ■ The transaction number within a single call leg is identified in the CSeq field. ■ The media capability User A is ready to receive is specified. ■ The port on which SIP Gateway 1 is prepared to receive the RTP data is specified.
3.	Call Proceeding—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Call Proceeding message to PBX A to acknowledge the Call Setup request.
4.	INVITE—SIP Proxy Server to SIP Gateway 2	The SIP proxy server checks whether its own address is contained in the Via field (to prevent loops), directly copies the To, From, Call-ID, and Contact fields from the request it received from SIP Gateway 1, changes the Request-URI to indicate the server to which it intends to send the INVITE request, and then sends a new INVITE request to SIP Gateway 2. In the INVITE request, the SIP proxy server also adds the Record-Route header to ensure that it is in the path of subsequent SIP requests for the same call leg. In the Record-Route field, the SIP proxy server adds its Request-URI.
5.	100 Trying—SIP Proxy Server to SIP Gateway 1	The SIP proxy server sends a 100 Trying response to SIP Gateway 1.
6.	Setup—SIP Gateway 2 to PBXB	SIP Gateway 2 receives the INVITE request from the SIP proxy server and initiates a Call Setup with User B via PBXB.
7.	100 Trying—SIP Gateway 2 to SIP Proxy Server	SIP Gateway 2 sends a 100 Trying response to the SIP proxy server. The SIP proxy server might or might not forward the 100 Trying response to SIP Gateway 1.
8.	Call Proceeding—PBX B to SIP Gateway 2	PBX B sends a Call Proceeding message to SIP Gateway 2 to acknowledge the Call Setup request.

Step	Action	Notes
9.	Alerting—PBX B to SIP Gateway 2	PBX B locates User B and sends an Alert message to SIP Gateway 2. The User B phone begins to ring.
10.	180 Ringing—SIP Gateway 2 to SIP Proxy Server	SIP Gateway 2 sends a 180 Ringing response to the SIP proxy server.
11.	180 Ringing—SIP Proxy Server to SIP Gateway 1	The SIP proxy server forwards the 180 Ringing response to SIP Gateway 1.
12.	Alerting—SIP Gateway 1 to PBX A	SIP Gateway 1 sends an Alert message to User A via PBX A. The Alert message indicates that SIP Gateway 1 has received a 180 Ringing response. User A hears the ringback tone that indicates that User B is being alerted. At this point, a one-way voice path is established between SIP Gateway 1 and PBX A and between SIP Gateway 2 and PBX B. A two-way RTP channel is established between SIP Gateway 1 and SIP Gateway 2.
13.	Connect—PBX B to SIP Gateway 2	User B answers the phone. PBX B sends a Connect message to SIP Gateway 2. The connect message notifies SIP Gateway 2 that the connection has been made.
14.	200 OK—SIP Gateway 2 to SIP Proxy Server	SIP Gateway 2 sends a 200 OK response to the SIP proxy server. The 200 OK response notifies the SIP proxy server that the connection has been made. In the 200 OK response, the SIP Gateway 2 adds the Record-Route header (received in the INVITE request) to ensure that it is in the path of subsequent SIP requests for the same call leg. If User B supports the media capability advertised in the INVITE message sent by the SIP proxy server, it advertises the intersection of its own and User A media capability in the 200 OK response. If User B does not support the media capability advertised by User A, it sends back a 400 Bad Request response with a 304 Warning header field. The SIP proxy server must forward 200 OK responses.
15.	200 OK—SIP Proxy Server to SIP Gateway 1	The SIP proxy server forwards the 200 OK response that it received from SIP Gateway 2 to SIP Gateway 1.
16.	Connect—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Connect message to PBX A. The Connect message notifies PBX A that the connection has been made.
17.	Connect ACK—PBX A to SIP Gateway 1	PBX A acknowledges the Connect message from SIP Gateway 1.
18.	ACK—SIP Gateway 1 to SIP Proxy Server	SIP Gateway 1 sends an ACK to the SIP proxy server. The ACK confirms that SIP Gateway 1 has received the 200 OK response from the SIP proxy server.
19.	ACK—SIP Proxy Server to SIP Gateway 2	Depending on the values in the To, From, CSeq, and Call-ID field, the SIP proxy server might process the ACK locally or proxy it. If the fields in the ACK match those in previous requests processed by the SIP proxy server, the server proxies the ACK. If there is no match, the ACK is proxied as if it were an INVITE request. The SIP proxy server forwards the SIP Gateway 1 ACK response to SIP Gateway 2.

Step	Action	Notes
20.	Connect ACK—SIP Gateway 2 to PBX B	SIP Gateway 2 acknowledges the Connect message from PBX B. The call session is now active. The two-way voice path is established directly between SIP Gateway 1 and SIP Gateway 2; not via the SIP proxy server. At this point, a two-way voice path is established between SIP Gateway 1 and PBX A and between SIP Gateway 2 and PBXB. A two-way RTP channel is established between SIP Gateway 1 and SIP Gateway 2.
21.	Disconnect—PBX B to SIP Gateway 2	After the call is completed, PBX B sends a Disconnect message to SIP gateway2. The Disconnect message starts the call session termination process.
22.	BYE—SIP Gateway 2 to SIP Proxy Server	SIP Gateway 2 sends a BYE request to the SIP proxy server. The BYE request indicates that User B wants to release the call. Because it is User B that wants to terminate the call, the Request-URI field is now replaced with the PBX A SIP URL and the From field contains the User B SIP URL.
23.	BYE—SIP Proxy Server to SIP Gateway 1	The SIP proxy server forwards the BYE request to SIP Gateway 1.
24.	Disconnect—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Disconnect message to PBX A.
25.	Release—SIP Gateway 2 to PBX B	After the call is completed, SIP Gateway 2 sends a Release message to PBX B.
26.	Release—PBX A to SIP Gateway 1	PBX A sends a Release message to SIP Gateway 1.
27.	200 OK—SIP Gateway 1 to SIP Proxy Server	SIP Gateway 1 sends a 200 OK response to the SIP proxy server. The 200 OK response notifies SIP Gateway 2 that SIP Gateway 1 has received the BYE request.
28.	200 OK—SIP Proxy Server to SIP Gateway 2	The SIP proxy server forwards the 200 OK response to SIP Gateway 2.
29.	Release Complete—PBX B to SIP Gateway 2	PBX B sends a Release Complete message to SIP Gateway 2.
30.	Release Complete—SIP Gateway 1 to PBX A	SIP Gateway 1 sends a Release Complete message to PBX A and the call session is terminated.

DTMF Relay Considerations

The topic describes possible issues with DTMF tones in a VoIP network that includes PSTN, PBXs and H.323 gateways.



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

An inability to break dial tone is a common problem encountered in a VoIP network. This is normally because the calling party is unable to pass the DTMF tones or digits to the terminating device, which prevents callers from dialing the desired extension or interacting with the device that needs DTMF tones (such as voice-mail or IVR applications). This problem could be caused by the following:

- DTMF tones are not being generated by the calling party's phone
- DTMF tones are not being understood by the terminating device
- DTMF tones are being passed but not understood because of distortion
- Other signaling and cabling issues

In the case of a VoIP call from an originating gateway (OGW) to a terminating gateway (TGW), terminating the call to a telephony device might not be understood. When passing DTMF tones through a compressed VoIP audio path, some or part of the dual tones could become slightly distorted because digital signal processor (DSP) codecs are designed to interpret human speech, not machine tones. Usually, such distortion does not occur with earlier compression codecs such as G732 or G711. However, later compression codecs may cause distortion of in-band tones.

H.323 DTMF Relay Considerations

Cisco.com

Cisco IOS Software Release 12.0(5)T supports four out-of-band DTMF transport methods:

- Cisco RTP sends tones in the RTP stream that are coded differently from voice.
- RTP NTE sends tones in the RTP stream as NSEs.
- H.245 alphanumeric sends tones as ASCII text characters.
- H.245 signal includes tone duration with the tone.

To send digits out-of-band, do the following:

- Enable the chosen method of DTMF relay under dial-peer configuration.
- The peer must indicate during call establishment that it is capable of receiving the DTMF option that is used.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-19

There are four methods for DTMF relay with H.323 gateways. One is an in-band, Cisco proprietary method, one is an in-band method using named signaling events, and the other two, available since Cisco IOS Release 12.0(5)T, are out-of-band methods. All four of these techniques use the H.245 capabilities exchange, which is part of H.323v2, to signal to the remote VoIP gateway that a DTMF tone has been received and that the remote VoIP gateway should regenerate it. These are the four methods:

- Cisco RTP with the **dtmf-relay cisco-rtp** command
- RTP Named Telephony Event (NTE) with the **dtmf-relay rtp-nte** command
- H.245 alphanumeric with the **dtmf-relay h245-alphanumeric** command
- H.245 signal with the **dtmf-relay h245-signal** command

Note H.245-alphanumeric is most typically used because it is required by the standard. H245 signal is optional and therefore may not be supported by other devices.

The ability of a gateway to receive DTMF digits in a particular format and the ability to send digits in that format are independent functions. The Cisco H.323 version 2 gateway is capable of receiving DTMF tones transported by any of these methods at all times. However, to send digits out-of-band using one of these methods, two conditions must be met.

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

Cisco Proprietary Mode

This method of DTMF relay provides a way to transport DTMF digits in an RTP voice stream by encoding them differently from the voice samples. The RTP digit events are encoded using a proprietary format similar to Frame Relay as described in the FRF.11 specification. The events are transmitted in the same RTP stream as non-digit voice samples, using payload type 121. To use the Cisco proprietary mode, Cisco gateways are required at both the originating and terminating endpoints of the call.

To enable the Cisco proprietary DTMF-relay mode, use the **dtmf-relay cisco-rtp** command in dial-peer configuration mode.

RTP NTE Mode

Using NTE to relay DTMF tones provides a standardized means of transporting DTMF tones in RTP packets according to section 3 of RFC 2833, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*. RFC 2833 defines formats of RTP NTE packets used to transport DTMF digits, hookflash, and other telephony events between two peer endpoints. With the NTE method, the endpoints perform per-call negotiation of the DTMF-relay method. They also negotiate to determine the payload type value for the NTE RTP packets.

To enable the Cisco proprietary DTMF-relay mode, use the **dtmf-relay rtp-nte** command in dial-peer configuration mode.

H.245 Alphanumeric and H.245 Signal

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

The **dtmf-relay h245-alphanumeric** command simply relays DTMF tones as ASCII characters. For instance, the DTMF digit 1 is transported as the ASCII character "1". There is no duration information associated with tones in this mode. When the Cisco H.323 gateway receives a DTMF tone using this method, the Cisco H.323 gateway generates the tone on the PSTN interface of the call using a fixed duration of 500 ms. All H.323 version 2-compliant systems are required to support the "h245-alphanumeric" method, while support of the "h245-signal" method is optional.

The H.245 Signal DTMF Relay feature supports keypad-initiated applications. The **dtmf-relay h245-signal** command relays a more accurate representation of a DTMF digit than does the **dtmf-relay h245-alphanumeric** command because tone duration information is included along with the digit value. This information is important for applications requiring that a key be pressed for a particular length of time. For example, one popular calling card feature allows the caller to terminate an existing call by pressing the # key for more than two seconds and then making a second call without having to hang up in between. This feature is beneficial because the caller does not have to dial the access number and personal identification number (PIN) code again. Outside-line access charges, which are common at hotels, may also be avoided.

DTMF relay can be turned off, and DTMF tones can be sent in-band by using the **no dtmf-relay** version of the command in Cisco IOS in dial-peer configuration mode.

Note If none of these options is selected, DTMF tones are transported in-band. Likewise, if the peer is not capable of receiving DTMF in any of the modes that were enabled, DTMF tones are sent in-band. When the Cisco H.323 version 2 gateway is involved in a call to a Cisco gateway that is running a version of Cisco IOS software prior to Release 12.0(5)T, DTMF tones are sent in-band because those systems do not support DTMF relay.

Example: dtmf-relay cisco-rtp Command

Cisco.com

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

```
dtmf-relay cisco-rtp
```

- **Multiple DTMF relay options can be configured on one dial peer.**

```
router(config)#dial-peer voice 100 voip
router(config-dial-peer)#destination-pattern 555...
router(config-dial-peer)# session target ipv4:10.1.1.1
router(config-dial-peer)# CODEC g729ar8
router(config-dial-peer)# dtmf-relay cisco-rtp h245-signal
router(config-dial-peer)# ip precedence 5
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-20

The screen capture is an example out-of-band DTMF configuration on a Cisco IOS gateway. The command to enable Cisco proprietary RTP is highlighted in the screen capture.

You would configure similarly all four of the out-of-band DTMF-relay options . Simply replace the **dtmf-relay cisco-rtp** command with the appropriate alternative.

You can enable more than one DTMF-relay option for a particular dial peer, to support multiple destinations that might use different methods. If you enable more than one option, and if the peer is capable of receiving DTMF in more than one of these formats, the router selects the DTMF format with the highest priority. The priority for DTMF relay is as follows:

4. Cisco RTP (highest priority)
5. RTP NTE
6. H.245 signal
7. H.245 alphanumeric
8. None. DTMF is sent as in-band voice

For more information about H.323 DTMF-relay Cisco-RTP configuration, see the Solution 4 section of “Inability to Break Dialtone in a Voice over IP Network” at <http://www.cisco.com/warp/public/788/unable-break-dialtone.html>.

For more information on configuring multiple DTMF-relay options on a particular dial peer, see “H.323 Dual Tone Multifrequency Relay Using Named Telephone Events” at http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800b5e46.html.

MGCP DTMF Relay Considerations

Cisco.com

Cisco supports MGCP DTMF transport in three ways:

- Cisco proprietary mode
- NSE mode
- MGCP out-of-band mode

The following are notes on MGCP DTMF relay:

- The best practice is to use NSE mode.
- Configure selected mode in Cisco IOS global configuration mode.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-21

Cisco supports MGCP DTMF transport in three ways:

- Cisco proprietary mode
- Named Signaling Event (NSE) mode:
 - MGCP-based DTMF relay: Gateway-controlled mode
 - MGCP-based DTMF relay: Call agent-controlled mode
- MGCP out-of-band DTMF relay

Cisco Proprietary Mode

The Cisco proprietary method has already been discussed with H.323. However since dial peers are normally not used on an MGCP gateway, the configuration of this method happens in the global configuration mode with the **mgcp dtmf-relay codec {all | low-bit-rate} mode cisco** command. To disable this process for uncompressed codecs, use the **no mgcp dtmf-relay voip** form of this command.

NSE Mode

Similar to the Cisco proprietary mode, MGCP-based DTMF relay sends digits in an RTP stream. However, for this mode, support is added for RFC 2833, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*. Support of RFC 2833 is standards-based and allows greater interoperability with other gateways and call agents.

In this method, each DTMF digit is encoded as a RTP NTEs packet, which is transmitted and received, whereas digit samples usually are carried in voice packets. The named events are sent as RTP packets over UDP. The packets are encoded with a payload type that is negotiated during connection establishment between the gateways using SDP.

MGCP-based DTMF relay provides two modes of implementation:

- In gateway-controlled mode, gateways negotiate DTMF transmission by exchanging capability information in SDP messages. That transmission is transparent to the call agent. Gateway-controlled mode allows use of the DTMF-relay feature without upgrading the call agent software to support the feature.
- In call agent-controlled mode, call agents use MGCP messaging to instruct gateways to process DTMF traffic.

To configure this method of DTMF relay, use the **mgcp dtmf-relay codec {all | low-bit-rate} mode {nte-gw | nte-ca}** command in global configuration mode where **nte-gw** and **nte-ca** are the triggers for gateway-controlled mode or call agent-controlled mode respectively.

The following lists the benefits of MGCP-based DTMF:

- There is MGCP support for RFC 2833, RTP payload for DTMF digits, telephony tones, and telephony signals.
- DTMF relay is more reliable.
- There is a greater interoperability with third-party equipment.
- Gateway-controlled and call agent-controlled modes allow for phased network upgrades.

Note The only restriction on MGCP NSE-mode DTMF relay is that DTMF relay supports the dynamic RTP payload range of 98 to 119 .

If DTMF relay is not configured, the DSPs on the gateways send and receive DTMF digits in-band in the voice codec.

MGCP Out-of-band DTMF Relay

Within the MGCP protocol is the concept of packages. The MGCP gateway loads the DTMF package on start-up. The MGCP gateway sends symbols over the control channel to represent any DTMF tones it receives. Cisco CallManager then interprets these signals and passes on the DTMF signals, out-of-band, to the signaling endpoint. MGCP digit events are sent using NOTIFY messages to the call agent, which plays them on the remote gateway using RQNT messages with signal playout request.

If either the Cisco proprietary mode or the NSE mode is used, each gateway is unaware of the remote gateway DTMF-relay configuration because it is not indicated in the SDP. Each side determines whether to use DTMF relay based on its locally configured mode setting and a combination of voice codec and codec filter settings. Each side uses its locally configured RTP payload type when encoding RTP named event packets.

Interoperability of endpoints relies on matching command-line interface (CLI) configurations. The value used for NSE mode is configured using the **mgcp tse payload** command. The payload type for Cisco proprietary mode is 121. This value is used regardless of the configured payload value.

In MGCP out-of-band mode, the call agent uses MGCP control commands to keep both gateways informed of DTMF requirements.

To configure MGCP out-of-band DTMF relay, use the **mgcp dtmf-relay voip codec {all | low-bit-rate} mode out-of-band** command in global configuration mode.

Note Cisco Catalyst 6000, Cisco Digital Gateway DE-30+, and Cisco Digital Gateway DT-24+ all support MGCP with Cisco CallManager Release 3.1 and later. DTMF relay is enabled by default and does not need additional configuration.

Summary of DTMF Relay Configuration Commands

Command	Description
<pre>mgcp dtmf-relay voip codec {all low-bit- rate} mode {cisco nse out-of-band nse-gw nse-ca }</pre>	<p>all: Dual tone multifrequency (DTMF) relay is to be used with all voice codecs.</p> <p>low-bit-rate: DTMF relay is to be used with only low-bit-rate voice codecs, such as G.729.</p> <p>cisco: RTP digit events are encoded using a proprietary format similar to Frame Relay as described in the FRF.11 specification. The events are transmitted in the same RTP stream as nondigit voice samples, using payload type 121.</p> <p>nse: RTP digit events are encoded using the format specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples, using the payload type that is configured using the mgcp tse payload command.</p> <p>out-of-band: MGCP digit events are sent using NTFY messages to the call agent, which plays them on the remote gateway using RQNT messages with S: (signal playout request).</p> <p>nse-gw: RTP digit events are encoded using the NTE format specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples. The payload type is negotiated by the gateways before use. The configured value for payload type is presented as the preferred choice at the beginning of the negotiation.</p> <p>nse-ca: Identical to the nse-gw keyword behavior except that the call agent local connection options a: line is used to enable or disable DTMF relay.</p> <p>Defaults</p> <p>For the Cisco 7200 series router, the command is not enabled. For all other platforms, noncompressed codecs are disabled.</p> <p>Usage Guidelines</p> <p>Use this command to access an announcement server or a voice-mail server that cannot decode RTP packets containing DTMF digits. When the mgcp dtmf-relay command is active, the DTMF digits are removed from the voice stream and carried so that the server can decode the digits.</p> <p>Only VoIP supports the mode keyword for forwarding digits on codecs.</p> <p>You must enter additional configuration parameters in the Cisco CallManager MGCP gateway configuration interface.</p>

Example: MGCP DTMF Relay Out-of-Band

Cisco.com

```
mgcp
mgcp call-agent 10.3.64.1 service-type mgcp version 0.1
mgcp modem relay voip mode nse
mgcp modem relay voip gateway-xid
no mgcp timer receive-rtcp
mgcp dtmf-relay codec all mode out-of-band
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 1001 pots
  application mgcpapp
  port 3/0:0
!
dial-peer voice 1002 pots
  application mgcpapp
  port 3/0:1
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0—1.22

The figure shows an example out-of-band DTMF-relay configuration on a Cisco IOS gateway

The command **out-of-band** can be switched for **cisco**, **nse-gw**, or **nse-ca**.

For more information, see *MGCP Based Fax (T.38) and DTMF Relay* at http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087eb3.html.

SIP DTMF Relay Considerations

Cisco.com

- **SIP DTMF relay is configured in dial-peer configuration mode. There are two methods:**
 - **RTP NTE: Forwards DTMF tones by using RTP with the NTE payload type**
 - **SIP NOTIFY: Forwards DTMF tones using SIP NOTIFY messages**
- **If SCCP IP phones are deployed, use SIP NOTIFY.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-23

The SIP DTMF-relay method is needed in the following situations:

- When SIP is used to connect a Cisco SRST system to a remote SIP-based IVR or voice-mail application
- When SIP is used to connect a Cisco SRST system to a remote SIP PSTN voice gateway that goes through the PSTN to a voice-mail or IVR application

Note The need to use out-of-band DTMF-relay conversion is limited to SCCP phones. SIP phones natively support in-band DTMF relay as specified in RFC 2833.

Use the commands in the “DTMF Relay SIP Commands” table to specify how to configure SIP gateway relay tones.

SCCP IP phones do not support in-band DTMF digits. They are capable only of sending out-of-band DTMF digits. To support SCCP devices, originating and terminating SIP gateways can use Cisco proprietary NOTIFY-based out-of-band DTMF relay. In addition, NOTIFY-based out-of-band DTMF relay can also be used by analog phones attached to analog voice ports (FXS) on the router.

NOTIFY-based out-of-band DTMF relay sends messages bidirectionally between the originating and terminating gateways for a DTMF event during a call. If multiple DTMF-relay mechanisms are enabled on a SIP dial peer and are negotiated successfully, NOTIFY-based out-of-band DTMF relay takes precedence.

The originating gateway sends an INVITE message with SIP Call-Info header to indicate the use of NOTIFY-based out-of-band DTMF relay. The terminating gateway acknowledges the message with an 18x or 200 Response message, also using the Call-Info header. Whenever a DTMF event occurs, the gateway sends a SIP NOTIFY message for that event after the SIP INVITE and 18x or 200 Response messages negotiate the NOTIFY-based out-of-band DTMF-relay mechanism. In response, the gateway expects to receive a 200 OK message.

The NOTIFY-based out-of-band DTMF-relay mechanism is similar to the DTMF message format described in RFC 2833.

For more detailed information, refer to *SIP Gateway Enhancements*, Cisco IOS Software Release 12.2(15)ZJ found at:

<http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5012/ps5049/index.html>.

You must use these commands on both originating and terminating gateways:

- **dial-peer voice *tag* voip**
- **dtmf-relay sip-notify**
- **exit**
- **sip-ua**
- **notify telephone-event max-duration *time***
- **exit**

DTMF Relay SIP Commands

Command	Description
<code>dtmf-relay (Voice over IP)</code>	Use this command to specify how a SIP gateway relays DTMF tones between telephony interfaces and an IP network.
<code>dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal] [rtp-nte] [sip-notify]</code>	Use this command to specify how an H.323 or SIP gateway relays DTMF tones between telephony interfaces and an IP network. Use the dtmf-relay command in dial-peer configuration mode. To remove all signaling options and to send the DTMF tones as part of the audio stream, use the no form of this command.
<code>no dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal] [rtp-nte] [sip-notify]</code>	<p><i>cisco-rtp</i>: (Optional) This command element forwards DTMF tones using RTP with a Cisco proprietary payload type.</p> <p><i>h245-alphanumeric</i>: (Optional) This command element forwards DTMF tones using the H.245 alphanumeric User Input Indication method and it supports tones from 0 to 9, *, #, and from A to D.</p> <p><i>h245-signal</i>: (Optional) This command element forwards DTMF tones using the H.245 signal User Input Indication method and it supports tones are from 0 to 9, *, #, and from A to D.</p> <p><i>rtp-nte</i>: (Optional) This command element forwards DTMF tones by using RTP with the NTE payload type.</p> <p><i>sip-notify</i>: (Optional) This command element forwards DTMF tones using SIP NOTIFY messages.</p>

Example: SIP DTMF Relay

Cisco.com

Example: Out-of-band to in-band SIP DTMF relay

```
dial-peer voice 1 voip
destination-pattern 2000
session protocol sipv2
session target ipv4:10.4.175.2
dtmf-relay rtp-nte
codec g711ulaw
```

Example: NOTIFY-based DTMF relay

```
dial-peer voice 123 voip
destination-pattern [12]...
monitor probe icmp-ping
session protocol sipv2
session target ipv4:10.8.17.42
dtmf-relay sip-notify
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1.24

The top example in the figure shows an out-of-band to in-band DTMF-relay SIP gateway configuration example. The commands that identify this configuration as a SIP configuration and that enable the DTMF-relay feature are highlighted in the figure.

The bottom example in the figure shows a notify-based DTMF-relay configuration example. The commands that identify this configuration as a SIP configuration and that enable notify-based DTMF-relay feature are highlighted in the figure.

Note The **show sip-ua status** command output shows the time interval between consecutive NOTIFY messages for a telephone event. The figure does not show that the time interval is 2000 ms.

DTMF Relay Configuration Options for All VoIP Call Control Protocols

Type of Signaling	DTMF Relay Mode	Example DTMF Relay Commands	H.323	MGCP	SIP
In-Band	Cisco Proprietary	<code>dtmf-relay cisco-rtp</code> or <code>mgcp dtmf-relay codec all mode cisco</code>	X	X	
	RTP NTE	<code>dtmf-relay rtp-nte</code>	X		X
	MGCP-Based NSE Mode	<code>mgcp dtmf-relay codec all mode nte-gw</code>		X	
		<code>mgcp dtmf-relay codec all mode nte-ca</code>			X
Out-of-Band	H.245 Alphanumeric	<code>dtmf-relay h245-alphanumeric</code>	X		
	H.245 Signal	<code>dtmf-relay h245-signal</code>	X		
	MGCP Out-of-Band	<code>mgcp out-of-band</code>		X	
	SIP NOTIFY	<code>dtmf-relay sip-notify</code>			X

Note H.323 and SIP DTMF-relay configurations are done in dial-peer mode. MGCP DTMF-relay configurations are done in global configuration mode.

Choosing a Gateway Protocol

This topic describes the criteria for selecting one gateway protocol over other gateway protocols.

Choosing H.323

Cisco.com

Why Choose H.323?

- **Integrated access**
- **Fractional PRI support**
- **Caller ID support on analog FXO**
- **Many more TDM interface types and signaling**
- **Dropping DSPs on hairpinned calls**
- **Gateway-resident applications like TCL and VXML**
- **CAC network design with H.323 gatekeepers**
- **No release dependencies between gateways and Cisco CallManager**
- **Much easier migration architecture to SIP**
- **Call preservation for Cisco SRST**
- **NFAS support**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0—1-25

Using H.323 as the call control protocol to a gateway has the following advantages:

- H.323 provides integrated access. Data and voice channels can be placed on the same T1. For example, for a service provider like AT&T, FR and PRI can be placed on the same T1.
- H.323 provides support for fractional PRI.
- Gateways support caller ID on FXO ports. CallManager does not support caller ID on FXO ports from MGCP gateways.
- Many more TDM interface types and signaling protocols—for example, analog-Direct Inward Dialed (DID), receive and transmit (E&M), T1 Feature Group-D (FGD), and E1 R2—can be used.
- H.323 drops DSPs on hairpinned calls to enable capabilities like ISDN video switching.
- Gateway resident applications like Toolkit Command Language (TCL) and voice extensible markup language (VXML) can be used. TCL and VXML applications provide IVR features and call control functionality such as call forwarding, conference calling, and voice mail.
- CAC network design with H.323 gatekeepers is often necessary when voice and video coexist in a network and Cisco CallManager is not the only call controller in the network.
- There are no release dependencies between gateways and Cisco CallManager for supporting new voice hardware. New hardware cards on Cisco IOS gateways become immediately available for use with all existing Cisco CallManager releases.
- H.323 enables a much easier migration architecture to SIP because the fundamental concepts of H.323 and SIP—for example, distributed control with dial-peer configurations—are the same.
- Calls from IP phones through an H323 gateway are dropped on a CallManager failover unless SRST mode is enabled. With SRST enabled, the calls are preserved.

Choosing MGCP

Cisco.com

Why choose MGCP?

- **Provides centralized management and control**
- **Better feature interaction with capabilities like caller ID**
- **Easy, centralized dial plan management**
- **Gateway voice security features as of Cisco IOS Release 12.3(5)T**
- **Supports QSIG supplementary services with Cisco CallManager**
- **Enhanced call survivability**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1.28

Using MGCP as the call control protocol to a gateway has the following advantages:

- Centralized configuration, control, and download from Cisco CallManager
- Better feature interaction with capabilities like caller ID and name display
- Easy, centralized dial-plan management
- Gateway voice security features (voice encryption) as of Cisco IOS Software Release 12.3.(5th)T
- Q Signaling (QSIG) supplementary services as supported by Cisco CallManager:
 - Cisco CallManager interconnects to a QSIG network using an MGCP gateway and T1 or E1 PRI connections to a private integrated services network (PISN). The MGCP gateway establishes the call connections. Using the PRI backhaul mechanism, the gateway passes the QSIG messages to the Cisco CallManager to set up QSIG calls and send QSIG messages to control features.
 - When a PBX is connected to a gateway that is using QSIG via H.323, calls that are made between phones on the PBX and IP phones attached to the Cisco CallManager can have only basic PRI functionality. The gateway that terminates the QSIG protocol provides only the calling line ID (CLID) and DID number, instead of Cisco CallManager providing that information.
- Enhanced call survivability:
 - Calls from IP phones through an MGCP gateway are preserved on a CallManager failover. This feature avoids dropped calls when applying the monthly operating system service release on the Cisco CallManagers
 - In SRST mode, calls from IP phones through an MGCP gateway are preserved on MGCP fallback for calls on analog or CAS circuits. Calls on ISDN circuits are dropped on fallback.

Choosing SIP

Cisco.com

Why Choose SIP?

- **SIP is independent of the media used, which allows flexibility to initiate sessions for different media types.**
- **Intelligence is distributed to endpoints, not to a single call-control component.**
- **IETF derived SIP from HTTP, so it is easy for third-party developers to create applications for it.**
- **SIP provides graceful support of protocol extensions.**
- **SIP is independent of any security protocol.**
- **SIP is a peer-to-peer protocol not an IP-to-PSTN gateway control protocol like MGCP.**
- **SIP runs on top of several transport protocols, including UDP, TCP, and SCTP.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-27

SIP is a peer-to-peer, multimedia signaling protocol that integrates with other Internet services, such as e-mail, Web browsers, voice mail, instant messaging, multiparty conferencing, and multimedia collaboration. When used with an IP infrastructure, SIP helps to enable rich communications with numerous multivendor devices and media. SIP can set up individual voice or conference calls, videoconferences and point-to-point video-enabled calls, Web collaboration and chat sessions, or instant messaging sessions between any number of SIP-enabled endpoints including IP phones, PCs, laptops, personal digital assistants (PDAs), and cell phones.

SIP is attractive as a signaling standard because it can connect and control communication sessions between applications, independent of media type or the function performed by the end applications. SIP is known as a “methods-based” signaling protocol because it provides the methods to connect, signal, and control sessions. In that sense, SIP is quite different from a “functionally based” signaling protocol, such as QSIG, which is used not only to establish sessions, but also to define the specific features those sessions can support.

The distinction between SIP and a functionally based signaling protocol is important because it greatly affects interoperability and flexibility. As a peer-to-peer protocol, the intelligence involved in SIP-enabled applications is distributed to endpoints and other components, not centralized in a single call-control component. New features can be added without upgrading infrastructure components such as proxy servers.

SIP is based on HTTP, so developers who are typically knowledgeable about HTTP and Web-based applications do not require intimate knowledge of the SIP infrastructure in order to write SIP-enabled applications. The common connection to HTTP opens up the application development process to third-party developers who can create targeted, vertically oriented applications. For example, internal users at a financial services company are likely to want features that are considerably different from those used by telemarketers in an outbound call center. SIP enables independent software vendors that have expertise in each market to develop applications specific to those areas. This type of open development environment represents a dramatic shift from the traditional TDM-based PBX paradigm discussed above. By opening up the application development process to more players, SIP promises to provide more innovation in less time and at less cost.

SIP also gracefully supports protocol extensions, so that applications can support advanced features and can still interoperate with other, less functional applications. Consider the following example. Three colleagues are on a conference call. Two of them are at a headquarters location where their SIP-enabled IP phones support video capabilities. The third is at a remote office that does not support video phones. SIP establishes the conference among the three users and enables the video portion for the two users whose equipment supports it. The third user participates in a traditional audio call. This is a shift from the “least-common denominator” approach in which only functions supported by all users are implemented (none of the colleagues would be able to use video).

In this way, SIP supports innovation within applications that can be combined, yet still works with similar applications that support features that have not been extended. In fact, SIP extensions define how SIP discovers the feature set each endpoint supports, and how SIP establishes each call accordingly.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **An H.323 gateway performs the following services in a VoIP network:**
 - Translation between audio, video, and data formats
 - Conversion between call setup signals and procedures
 - Conversion between communication control signals and procedures
- **The H.323 setup exchange using the Fast Connect abbreviated procedure reduces the number of round-trip exchanges by performing the capability exchange and logical channel assignments in one round trip.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—1-29

Summary (Cont.)

Cisco.com

- **DTMF relay solves the problem of DTMF distortion by transporting DTMF tones out-of-band or in-band in the RTP stream with different coding from the voice.**
- **SIP DTMF considerations include the need to think about out-of-band to in-band conversion.**
- **H.323 performs well in a TDM environment making it a good choice for migration.**
- **MGCP offers the advantage of powerful and scalable central call control.**
- **SIP is less mature than either H.323 or MGCP, but it offers developers the opportunity to build applications for SIP networks more easily than in other networks.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—1-30

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) Why is H.323 is considered to be an “umbrella protocol?” (Source: Overview of H.323 Gateways)

- Q2) How does H.323 interoperate with legacy voice networks? (Source: Overview of H.323 Gateways)

- A) H.323 is based on the H.225 standard, which interoperates with existing voice networks.
- B) H.323 uses the ISDN Q.931 protocol to interoperate with legacy voice networks.
- C) H.323 is based on the H.245 standard, which interoperates with existing voice networks.
- D) H.323 uses the EGIE, Phase 2 to interoperate with legacy voice networks.

- Q3) Which three services are performed by a H.323 gateway? (Choose three.) (Source: Overview of H.323 Gateways)

- A) translation between audio, video, and data formats
- B) registry maintenance of devices in the multimedia network
- C) conversion between call setup signals and procedures
- D) conversion between communication control signals and procedures
- E) bandwidth management and alternate gateway locating
- F) address translation and control access to legacy networks
- G) termination of all ISDN PRI Layer 2 (Q.921) signaling functions

- Q4) What does the Fast Connect procedure do in one round trip between H.323 gateways? (Source: H.323 Call Flow)

- A) establishes the capability exchange and logical channel assignments
- B) defaults the H.252 gateways to H.323 version 3 for all calls
- C) establishes rate-limit traffic by precedence
- D) establishes the capability exchange and codec assignments

- Q5) What are three of the benefits of the Cisco H.323 gateway? (Choose three.) (Source: Choosing a Gateway Protocol?)
- A) designed as a generic transaction protocol for session initiation
 - B) works well for organizations with centralized management and control
 - C) gateway resource availability reporting
 - D) shorter voice cut-through times
 - E) gateway fallback support Cisco CallManager
 - F) allows TDY users to communicate with voice users
 - G) gateway support for DTMF digit relay
- Q6) What two conditions must be met for a Cisco H.323 gateway to be able to send digits out-of-band? (Choose two.) (Source: H.323 DTMF Relay Considerations)
- A) A Cisco H.323 gateway has enabled the chosen method of DTMF relay under dial-peer configuration.
 - B) A Cisco H.323 gateway has enabled the chosen method of DTMF relay under global configuration.
 - C) The global dial peer must be configured so it is capable of receiving the forwarded digits from the remote end.
 - D) The dial peer must be configured so it is capable of receiving the DTMF option being used.
- Q7) Briefly describe how MGCP works. (Source: Overview of MGCP Gateways)
-
-
-
-
- Q8) What is an example of an MGCP call agent? (Source: Overview of MGCP Gateways)
- A) a H.323 gateway with MGCP enabled
 - B) the Cisco CallManager
 - C) a phone set up as an ACD (IPCC Express) phone agent
 - D) a desktop set up as an ACD (IPCC Express) agent (not Supervisor)
- Q9) How is voice data transmitted using MGCP? (Source: Choosing a Gateway Protocol)
- A) Voice data is transmitted using the RTP portion of the MGCP protocol.
 - B) Voice data is not transmitted via MGCP, only fax and modem tones are transmitted via MGCP.
 - C) Voice data is transmitted using the SIP portion of the MGCP protocol.
 - D) No voice data is transmitted through the MGCP protocol itself.

Q10) Is IETF support for the MGCP protocol a benefit? Briefly explain why or why not. (Source: Choosing a Gateway Protocol)

Q11) Why is it a benefit to transport DTMF tones out-of-band? (Source: DTMF Relay Considerations)

- A) The problem of DTMF distortion is solved.
- B) Fax tones are transported via TCP rather than as “voice” over UDP or RTP, which makes the transport of these tones very reliable.
- C) Dialed digits are transported in a separate carrier, like the D-channel of ISDN, thus conserving voice bandwidth.
- D) Dialed digits can code the “A”, “B”, “C”, and “D” tones provided for in the DTMF standard.

Q12) Explain the function of each type of peer in the SIP protocol. (Source: Overview of SIP Gateways)

Q13) What are the two types of SIP servers? (Choose two.) (Source: Overview of SIP Gateways)

- A) reversion server
- B) user agent server
- C) proxy server
- D) redirect server
- E) unified agent server
- F) universal proxy server
- G) registrar server
- H) registration server
- I) location server

Q14) What kind of transaction model is SIP based on? (Source: SIP Call Flow)

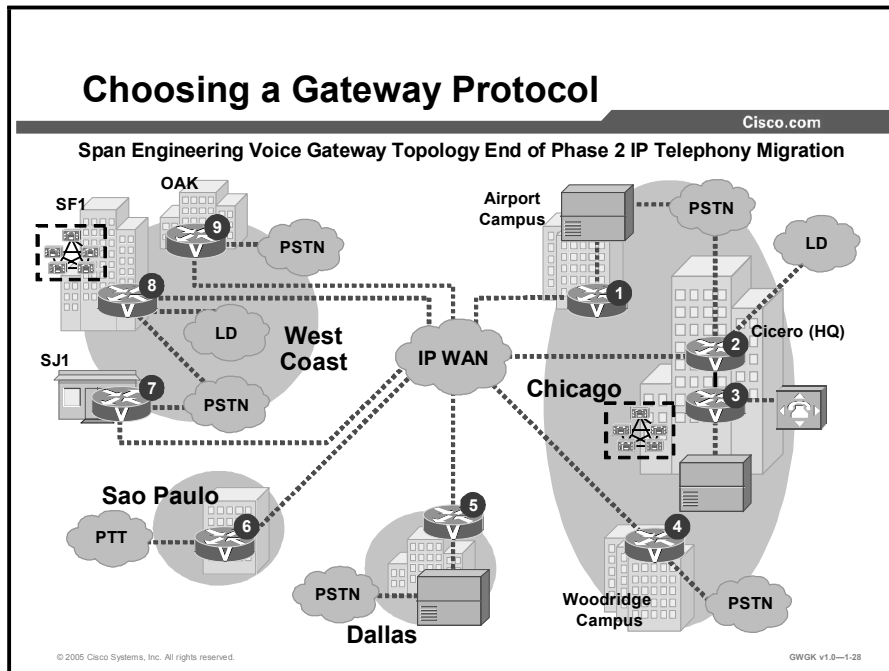
- A) a client-server model
- B) an HTTP-like request and response transaction model
- C) a primary agent–secondary agent model
- D) a peer-to-peer transaction model

Q15) Briefly explain what ensures SIP interoperability with H.323 and MGCP. (Source: Choosing a Gateway Protocol)

Q16) What does the out-of-band to in-band DTMF relay for Cisco IOS voice gateways feature enable? (Source: SIP DTMF Relay Considerations)

- A) support for the conversion of DTMF tones to counter the “distortion” found in voice-codes transporting dialed digits
- B) DTMF-relay communication between SIP devices and non-SIP endpoints using Cisco CallManager
- C) transcoding out-of-band tones into non G.711 audio codecs
- D) DTMF-relay to fax-relay communications between endpoints

Q17) In the Call Control Protocol column in the table below, write down the call control protocol (H.323, MGCP, or SIP) that you would choose for each gateway. The following information may help influence your selections: All PBX connections are T1 PRI-enabled and QSIG-enabled except Gateway 1, which connects with T1 CAS. SRST is enabled on Gateways 1, 4, 7, and 9. Cisco CallManager has not been deployed in Sao Paulo or Dallas. (Source: Choosing a Gateway Protocol)



Gateway Information

Gateway Number	Gateway Type	Gateway Connects To	Description	Call Control Protocol
1	2 x VVIC-2MFT-T1 in a 2811	Nortel Meridian Opt 11c	4 x T1 CAS	
2	1 x WS-6608-T1 1 x WS-SVC-CMM-6T1	PSTN Long Distance	8 x T1 PRI 5 x T1 PRI	
3	2 x VVIC-2MFT-T1 in a 3845 2 x NM-HDV-2T1-48 in a 3845	Avaya MV1.3 PBX Nortel Meridian 1	3 x T1 PRI 4 x T1 PRI	
4	2 x NM-HDV-2T1-48 in a 3845	PSTN	3x T1 PRI	
5	2 x NM-HDV-2T1-48 in a 3845	Avaya Definity G3si	3 x T1 PRI	
6	NM-HDV-2E1-60in a 3845	PTT PISN	1 x E1 R2 1 x E1 PRI	
7	VIC2-2BRI-NT/TE in a 2811	PSTN	2 x BRI	
8	4 ports on WS-6608-T1 4 ports on WS-6608-T1	PSTN Long Distance	4 x T1 PRI 4 x T1 PRI	
9	VVIC-1MFT-T1 in a 2821	PSTN	1 x T1 PRI	

Lesson Self-Check Answer Key

- Q1) H.323 is considered an “umbrella protocol” because it defines all aspects of call transmission, including call establishment, capabilities exchange, and network resource availability
- Q2) B
- Q3) A, C, D
- Q4) A
- Q5) A, C, G
- Q6) A, D
- Q7) MGCP is defined under RFC 2705. It is a plain text protocol that uses a master-slave relationship to fully control a gateway and its associated ports. The plain-text commands are sent to gateways, from call agents using UDP port 2427. Port 2727 is used to send messages from the gateways to the call agent.
- Q8) B
- Q9) C
- Q10) Yes, it can be a benefit. Without being subject to the rigors of the ITU-T procedures and policies, the IETF can respond quickly to user demands, although the solutions can be less mature than those created by the ITU-T.
- Q11) A
- Q12) The user agent client is a client application that initiates a SIP request and the user agent server is a server application that contacts the user when a SIP invitation is received and then returns a response on behalf of the user to the invitation originator.
- Q13) B, D
- Q14) B
- Q15) Although SIP messages are not directly compatible with H.323 and MGCP, these protocols can coexist in the same packet telephony network if a device that supports the interoperability is available.
- Q16) B
- Q17) H.323, MGCP, H.323, H.323, H.323, H.323, H.323 or SIP, MGCP, H.323 or SIP

Lesson 3

Implementing Gateways

Overview

After you have selected a gateway protocol, you can deploy the gateway. Again, this lesson discusses the three types of gateways: H.323, MGCP, and SIP. You will use your knowledge of these gateways to implement your own voice gateway procedures.

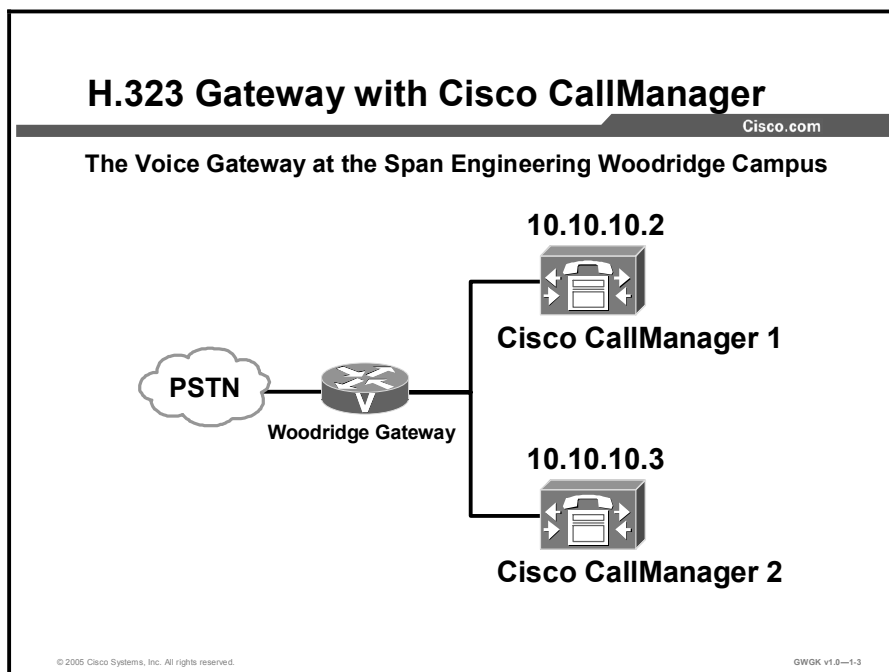
Objectives

Upon completing this lesson, you will be able to explain the problems with implementing voice gateways in support of IP telephony solutions. This ability includes being able to meet these objectives:

- Configure an H.323 gateway to integrate with Cisco CallManager
- Configure an H.323 gateway for toll bypass
- Diagram the basic MGCP gateway configurations for dial-peers and integration with the PSTN and PBXs
- Describe MGCP-controlled backhauling
- Explain the procedure for the basic configuration of a SIP gateway for VoIP support
- Explain how SIP gateways integrate with Cisco CallManager and Cisco CallManager Express in an IP telephony network

H.323 Gateway Integration with Cisco CallManager

The topic describes how to configure an H.323 gateway to integrate with Cisco CallManager.



The figure shows two Cisco CallManagers supporting one Cisco 2610 Router connected to a public switched telephone network (PSTN). In this topology, the Cisco CallManagers are functioning as a centralized call agent for managing a VoIP network. Cisco CallManager provides a scalable, distributable, and highly available enterprise IP telephony call-processing solution. Multiple Cisco CallManager servers are clustered and managed as a single entity.

Configure Voice-Enabled Router as an H.323 Gateway

Cisco.com

1. **Issue the voice class h323 1 command to set the H.225 timer to 3 seconds.**

```
WDGGW#(config) voice class h323 1
WDGGW#(config) h225 timeout tcp establish 3 !--- Set
the timeout to 3 seconds.
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-1.4

There are two steps required to configure a Cisco IOS voice-enabled router as an H.323 gateway.

The first step is to decrease the H.225 timer on the H.323 gateway to 3 seconds. This step is necessary because by default, the H.225 timer that controls redirection to a less preferred dial peer on a “no-response” failure is considerably longer than the 10-second timer of the Q.931 Call Proceeding timer. If a call comes in to an H.323 gateway through an ISDN trunk and is forwarded to an inoperative Cisco CallManager, the router waits for about 40 seconds before attempting to use a dial peer with a lower preference, or before clearing the call. By the time this occurs, the ISDN Q.931 signaling on the H.323 gateway has already sent an ISDN Q.931 CALL DISCONNECT message to the ISDN switch. The router provides an ISDN clearing code of 0x8066, which is “recovery on timer expiry.”

It is not possible for the H.323 gateway to reset the Call Proceeding timer because it is attempting to use a different dial-peer. Therefore, the H.323 gateway must switch peers and complete the call using the secondary Cisco CallManager server within the 10 seconds allowed by the Q.931 (Incoming Call Proceeding) timer.

By setting the H.225 timer to 3 seconds, the router attempts a connection to the primary Cisco CallManager server. If it does not receive a response in 3 seconds, it falls back to the secondary Cisco CallManager server.

Configure a Voice-Enabled Router as an H.323 Gateway (Cont.)

Cisco.com

2. Configure dial-peer statements.

```
WDGGW(config)#dial-peer voice 4 voip
WDGGW(config)dial-peer)#destination-pattern 4...
WDGGW(config)dial-peer)#session target ipv4:10.10.10.2
WDGGW(config)dial-peer)#codec g711ulaw
WDGGW(config)dial-peer)#dtmf-relay h245alphanumeric
!
WDGGW(config)#dial-peer voice 1 pots
WDGGW(config)dial-peer)#destination-pattern 9T
WDGGW(config)dial-peer)#direct-inward-dial
WDGGW(config)dial-peer)#port 2/0:23
WDGGW(config)dial-peer)#incoming called-number .
```

- **This configuration routes incoming calls from the PSTN to any IP phone in the 4000 to 4999 range and all outbound calls to any number in the NANP.**
- **The voip dial-peer to CallManager 2 is shown in the following example.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1.5

The figure shows the configuration of two dial peers. These dial peers send calls to either Cisco CallManager 1 or the PSTN. The configuration of a second VoIP dial peer for CallManager 2 is not provided here but is shown in the figure “Configuration of a Voice-Enabled Router as an H.323 Gateway.”

A description of the commands used in the figure is provided in the “Commands Used to Configure H.323 Gateways with Cisco CallManager” table.

Commands Used to Configure H.323 Gateways with Cisco CallManager

Command	Description
WDGGW (config) # dial-peer voice 4000 voip	This command points the dial peer to the Cisco CallManager.
WDGGW (config-dial-peer) # destination-pattern 4...	This command routes anything with this pattern to the Cisco CallManager. The periods are wildcards, so they stand for 4000–4999.
WDGGW (config-dial-peer) # session target ipv4:10.10.10.6	Session target is the Cisco CallManager IP address.
WDGGW (config-dial-peer) # codec g711ulaw	Use this codec.
WDGGW (config-dial-peer) # dtmf-relay h245-alphanumeric	Use dual tone multifrequency (DTMF) relay to transport DTMF digits.
WDGGW (config-dial-peer) # incoming called-number 1234	This dial-peer command defines the called number destination or dialed number identification service (DNIS) string. When properly configured, the dial peer uses the called number to match the incoming call leg to an inbound dial peer.
WDGGW (config) # dial-peer voice 1 pots	The dial peer points the PRI trunk to PSTN.
WDGGW (config-dial-peer) # destination-pattern 9T	Route this pattern to the PSTN cloud through the T1/PRI. "T" is a wildcard for any digits.
WDGGW (config-dial-peer) # direct-inward-dial	Direct Inward Dialing (DID) does not generate a secondary dial tone on incoming calls from PSTN.
WDGGW (config-dial-peer) # port 2/0:23	This command defines the plain old telephone service (POTS) voice port through which calls to this dial peer are placed.

Example: Configuration of a Voice-Enabled Router as an H.323 Gateway

Cisco.com

```
WDGGW#(config) voice class h323 1
WDGGW#(config) h225 timeout tcp establish 3
WDGGW(config)#dial-peer voice 4 voip
WDGGW(config-dial-peer)#destination-pattern 4...
WDGGW(config-dial-peer)#session target ipv4:10.10.10.2
WDGGW(config-dial-peer)#preference 0
WDGGW(config-dial-peer)#voice-class h323 1
WDGGW(config-dial-peer)#dtmf-relay h245-alphanumeric
!
WDGGW(config)#dial-peer voice 5 voip
WDGGW(config-dial-peer)#destination-pattern 4...
WDGGW(config-dial-peer)#session target ipv4:10.10.10.3
WDGGW(config-dial-peer)#preference 1
WDGGW(config-dial-peer)#voice-class h323 1
WDGGW(config-dial-peer)#dtmf-relay h245-alphanumeric
!
WDGGW(config)#dial-peer voice 1 pots
WDGGW(config-dial-peer)#destination-pattern 9T
WDGGW(config-dial-peer)#direct-inward-dial
WDGGW(config-dial-peer)#port 2/0:23
WDGGW(config-dial-peer)#incoming called-number .
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1.6

In this example, the Cisco IOS router or gateway uses a T1 ISDN PRI trunk to the PSTN.

The configuration routes incoming calls from the PSTN to any IP phone in the range 4000 through 4999 via CallManager, and all outbound calls to any number in the North American Numbering Plan (NANP).

The “Configuration of a Cisco IOS H.323 Gateway” table shows a summary of the Cisco IOS software commands used to configure an H.323 gateway.

Configuration of a Cisco IOS H.323 Gateway

Command	Description
WDGGW# voice class h323 1	
WDGGW# h225 timeout tcp establish 3	Sets the timeout to 3 seconds
WDGGW (config) # dial-peer voice 4 voip	The dial peer pointing to the primary Cisco CallManager
WDGGW (config-dial-peer) # destination-pattern 4...	Routed this pattern to the Cisco CallManager
WDGGW (config-dial-peer) # session target ipv4:10.10.10.2	The primary Cisco CallManager IP address
WDGGW (config-dial-peer) # preference 0	
WDGGW (config-dial-peer) # voice-class h323 1	
WDGGW (config-dial-peer) # dtmf-relay h245-alphanumeric	
WDGGW (config-dial-peer) # incoming called-number 1234	
WDGGW (config) # dial-peer voice 5 voip	The dial peer pointing to the backup Cisco CallManager
WDGGW (config-dial-peer) # destination-pattern 4...	Routes this pattern to the Cisco CallManager
WDGGW (config-dial-peer) # session target ipv4:10.10.10.3	The backup Cisco CallManager IP address
WDGGW (config-dial-peer) # preference 1	
WDGGW (config-dial-peer) # dtmf-relay h245-alphanumeric	
WDGGW (config-dial-peer) # incoming called-number 1234	
WDGGW (config) # dial-peer voice 1 pots	The dial peer pointing to the PRI trunk to the PSTN
WDGGW (config-dial-peer) # destination-pattern 9T	Routes this pattern to the PSTN cloud through the T1/PRI
WDGGW (config-dial-peer) # direct-inward-dial	DID does not generate a secondary dial tone on incoming calls from PSTN.

H.323 Gateway Integration with Toll Bypass

This topic describes how to configure an H.323 gateway with toll bypass.

Toll Bypass

Cisco.com

A toll-bypass application allows users to bypass the PSTN and avoid paying toll charges because calls are routed over a packet network.

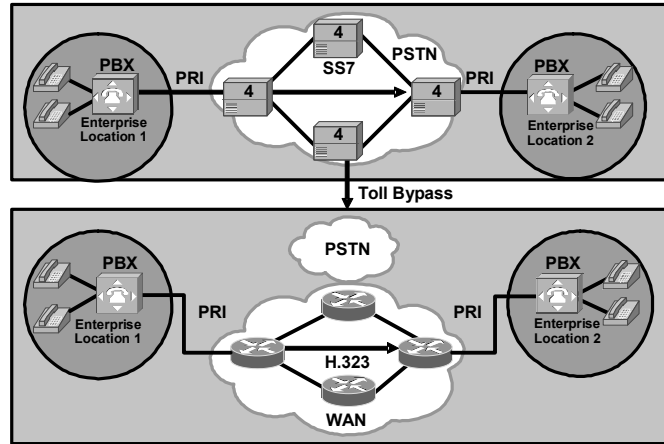
© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-1.7

A toll-bypass application allows users to bypass the PSTN and avoid paying toll charges by routing calls over a packet network.

The PSTN consists of the tandem time-division multiplexing (TDM)-based switches that use the packet network for long-distance (or toll) voice calls. Enterprise customers who typically depend on the PSTN for their interoffice voice traffic avoid toll charges by using the packet network with Cisco routers that serve as the edge voice gateways. Toll bypass allows some Internet service providers (ISPs) to offer residential customers free or very low-cost long-distance voice calls by routing the calls over the packet network.

Toll Bypass Topology

Cisco.com



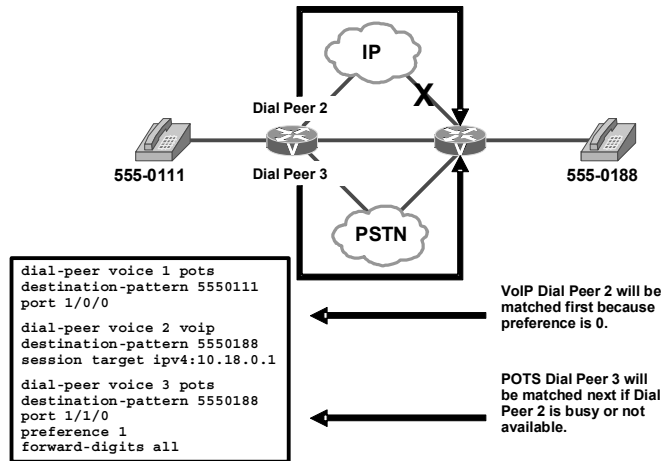
© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1.9

In the figure, traffic from the enterprise PBX enters the Cisco routers that serve as edge voice gateways. The edge voice gateways, in turn, route the call over the IP network using the H.323 protocol. As shown, the enterprise customers avoid the TDM-based toll switches for their interoffice voice traffic and rely on the packet network.

H.323 Toll Bypass Configuration Examples

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

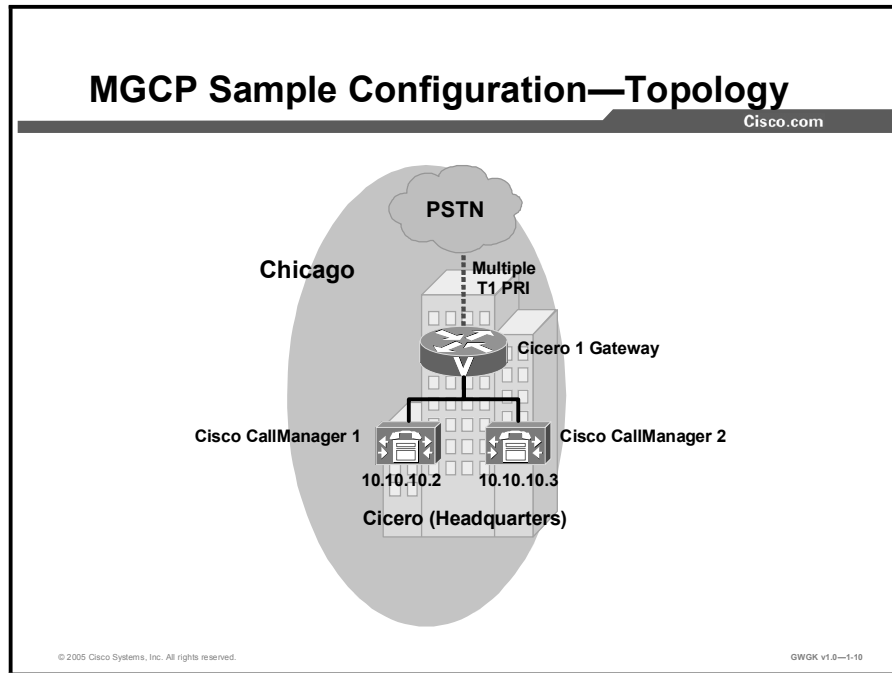
GWGK v1.0-1.9

Toll bypass is implemented in distributed call control environments. For example, H.323 or session initiation protocol (SIP) can be used for the call control protocol.

The distributed call routing intelligence in the gateway routers determines whether a call is destined for a site attached to the shared packet network (IP WAN) and first directs the call over the packet network (Dial Peer 2). If the packet network bandwidth is constrained, or the packet network is unavailable, the call is routed transparently to the PSTN gateway interface (Dial Peer 3) for transport to the remote site.

MGCP Gateway Integration with Cisco CallManager

This topic describes the basic Media Gateway Control Protocol (MGCP) gateway configurations for dial peers and integration with the PSTN and PBXs.



The figure illustrates gateway configuration. The topology consists of a Cisco 2620 Router running an MGCP call control protocol with PRI to the PSTN and an Ethernet connection to the Cisco CallManager call agent. The sample configuration shown in the following figures was generated using Cisco IOS Software Release 12.2(11)T.

Note This topic will use the information in the figure for the configuration examples in this topic.

Sample MGCP Configuration

Cisco.com

```
CTC1GW#show run
!--- Several lines of show output text deleted for brevity
mgcp
mgcp call-agent 10.10.10.2 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp modem passthrough voip mode cisco
mgcp sdp simple
mgcp package-capability rtp-package
mgcp package-capability sst-package
isdn switch-type primary-ni
call rsvp-sync
!
ccm-manager music-on-hold
!
ccm-manager mgcp
ccm-manager config server 10.10.10.2
ccm-manager config
!--- These three commands enable the trombone feature, which is
!--- the feature that lets CallManager control the gateway.
!
controller T1 1/0
framing esf
clock source internal
linecode b8zs
cablelength short 133
pri-group timeslots 1-24 service mgcp
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-11

The bolded commands in the screen capture show how to enable MGCP on a Cisco router and allow the Cisco CallManager to act as a call agent to control the gateway.

Sample MGCP Configuration (Cont.)

Cisco.com

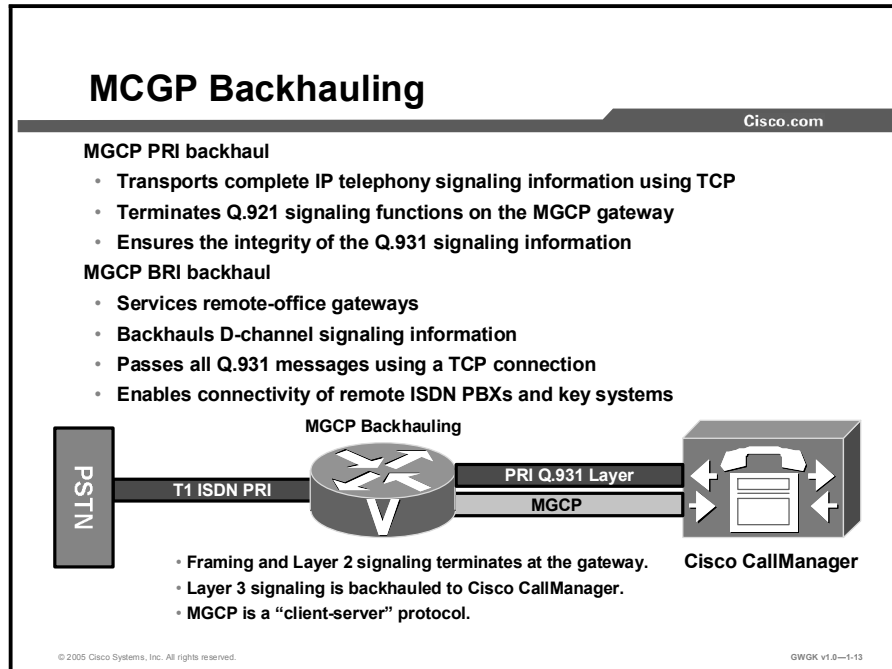
```
interface FastEthernet0/0
ip address 172.16.15.129 255.255.255.0
ip helper-address 172.16.15.10
no ip mroute-cache
duplex auto
speed auto
!
interface Serial1/0:23
no ip address
no logging event link-status
isdn switch-type primary-ni
isdn protocol-emulate network
isdn incoming-voice voice
isdn T310 10000
isdn bind-13 ccm-manager
no cdp enable
no ip http server
!
voice-port 1/0:23
!
dial-peer cor custom
!
dial-peer voice 9991023 pots
application mgcpapp
port 1/0:23
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-12

MGCP Backhauling

This topic provides an explanation of MGCP-controlled backhauling.



MGCP PRI backhaul is a method for transporting complete IP telephony signaling information from an ISDN PRI interface on a MGCP gateway to Cisco CallManager through a Transmission Control Protocol (TCP) connection. MGCP PRI backhaul terminates all of the ISDN PRI Layer 2 (Q.921) signaling functions on the MGCP gateway and packages all of the ISDN PRI Layer 3 (Q.931) signaling information into packets for transmission to Cisco CallManager through an IP tunnel. In this way, MGCP PRI backhaul ensures the integrity of the Q.931 signaling information that passes through the network for managing IP telephony devices.

The MGCP gateway also establishes a TCP link to the backup (secondary) Cisco CallManager server. In the event of a Cisco CallManager switchover, the secondary Cisco CallManager server performs the MGCP PRI backhaul functions. During the switchover, all active ISDN PRI calls are preserved, and the affected MGCP gateway is registered with the new Cisco CallManager server through a ReStart In Progress (RSIP) message. In this way, continued gateway operation is ensured.

MGCP-controlled backhaul of BRI signaling provides service to remote-office gateways that are connected by ISDN BRI trunks to a centralized Cisco CallManager. D-channel signaling information is backhauled to Cisco CallManager through a TCP session. All Q.931 messages are passed through the TCP connection between the Cisco MGCP gateway and Cisco CallManager. The feature enables you to connect remote ISDN PBXs and key systems to a Cisco ISDN BRI network termination (network side) or a PSTN Class 4 or Class 5 switch through a Cisco ISDN BRI terminal equipment (as user side) interface.

For more information, see *How to Configure MGCP with Digital PRI and Cisco CallManager* at

http://www.cisco.com/en/US/tech/tk652/tk701/technologies_configuration_example09186a00801ad22f.shtml.

MGCP Backhaul Configuration

Cisco.com

```
Router(config)# mgcp
Router(config)# mgcp call-agent 10.110.110.10 2427 service-type
mgcp version 0.1
Router(config)# mgcp dtmf-relay codec all mode out-of-band
Router(config)# controller t1 1/0
Router(config-controller)# pri-group timeslots 1-24 service mgcp
Router(config)# dial-peer voice 1 pots
Router(config-dial-peer)# application MGCPAPP
Router(config-dial-peer)# voice-port 1/0:23
Router(config)# interface serial 2/0:24
Router(config-line)# isdn switch-type type
Router(config-line)# isdn bind-L3 ccm-manager
Router(config)# ccm-manager MGCP
Router(config)# ccm-manager redundant-host 10.110.110.11
Router(config)# ccm-manager switchback graceful
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-15

The commands shown in the figure assume that a digital access PRI is in use. Descriptions of the commands used to configure MGCP backhaul are provided in the “MGCP Backhaul Configuration Commands” table.

MGCP Backhaul Configuration Commands

Command	Description
Router(Config)# mgcp	This command turns on MGCP.
Router(Config)# mgcp call-agent 10.110.110.10 2427 service-type mgcp version 0.1	The IP address is the Cisco CallManager, 2427 is the TCP port number, and service type defines either MGCP or SGCP and the version number.
Router(Config)# mgcp dtmf-relay codec all mode out-of-band	This command selects the codec type and the DTMF option.
Router(config)# controller tl 1/0 Router(config-controller)# pri-group timeslots 1-24 service mgcp	This command tells the gateway to use ports 1 to 24 of the PRI for service MGCP. The D channel will be port 23 and the actual channels will be 0 to 22.
Router(config)# dial-peer voice 1 pots	This command creates a plain old telephone service (POTS) dial peer that points to the D channel of the PRI, as seen in the command following the next. One is a random number selected for this example.
Router(config-dial-peer)# application MGCPAPP	This command turns on MGCP for the dial peer.
Router(config-dial-peer)# voice-port 1/0:23	This tells the dial peer to use this port for calls controlled by MGCP; it binds the port to MGCP.
Router(config)# interface serial 2/0:24	This command enters serial configuration mode for the ISDN port.
Router(config-line)# isdn switch-type type	This command specifies the ISDN switch type.
Router(config-line)# isdn bind-L3 ccm-manager	This command enables ISDN to backhaul Q.931. The Layer 3 information (Q.931 and above) is transported over TCP to the MGCP call agent which is Cisco CallManager in this case.
Router(config)# ccm-manager MGCP	This command allows the gateway to talk to the Cisco CallManager using MGCP.
Router(Config)# ccm-manager redundant-host 10.110.110.11	This command configures redundant Cisco CallManager for MGCP.
Router(Config)# ccm-manager switchback graceful	After the primary Cisco CallManager comes back on line, this command waits until any active calls are completed before the phones are registered back to the primary Cisco CallManager. Other options are immediate. You can also set a specific time for the phones to switch back.

Implementing a SIP Gateway

This topic describes the procedure for basic configuration of a SIP gateway for VoIP support.

Implementing a SIP Gateway

Cisco.com

Proposed SIP Topology for Span Engineering West Coast Location

SIP Configuration Task List

Step	Action
1	Configure SIP support for VoIP dial peers
2	(Optional) Change configuration of the SIP user agent
3	(Optional) Configure SIP call transfer
4	(Optional) Configure gateway accounting

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-1-16

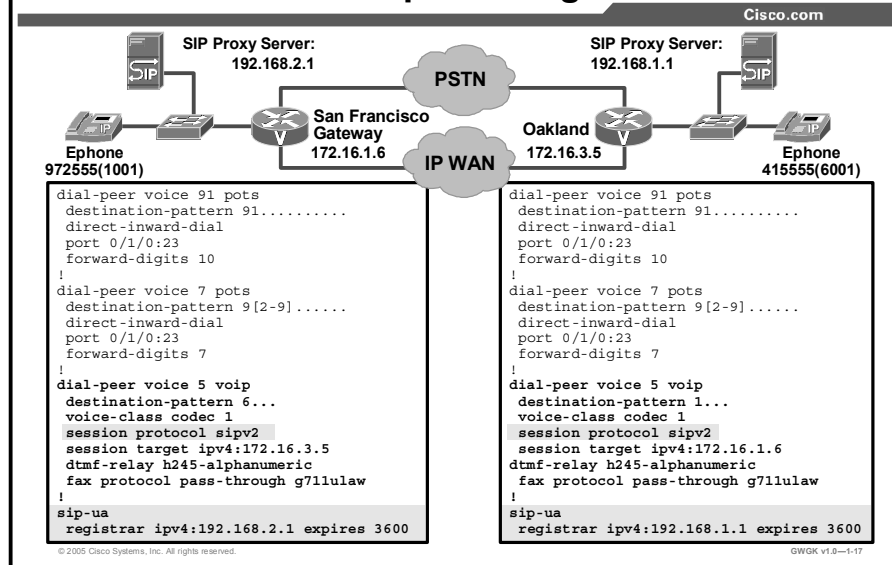
When implementing a SIP gateway, the standard prerequisite tasks for any type of voice gateway need to be performed, such as configuring VoIP as described in http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/1751/1751swg/config.htm. Once that is done, the steps described in the SIP Configuration Task List can be performed.

Note In this course, you will learn about Steps 1 and 2. Details on the other steps can be found at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvfax_c/vfvsip.htm#wp1094455.

The latest configuration commands for SIP gateways are listed in the *Cisco IOS SIP Configuration Guide* for Cisco IOS Release version 12.3(7)T, which can be found at http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a0080392125.html.

The configuration steps described in this topic are for a SIP gateway configuration. There is no distinction between an implementation with an H.323 network, a SIP network, or an MGCP network.

SIP Dial-Peer Sample Configuration



This example shows the configuration of the VoIP dial peers to support SIP and shows the change to the user agent configuration. Those commands specifically related to SIP configuration, for both gateways shown in the figure, are highlighted in the figure.

To configure SIP support for a VoIP dial peer, use the following commands beginning in global configuration mode.

Dial-Peer Configuration Commands

Step	Command	Purpose
1.	Router(config)# dial-peer voice <i>number</i> voip	Enters dial-peer configuration mode to configure a VoIP dial peer.
2.	Router(config-dial-peer)# session transport {udp tcp}	Enters the session transport type for the SIP user agent. The default is udp. The transport protocol (udp or tcp) specified with the session transport command must be identical to the protocol specified with the transport command.
3.	Router(config-dial-peer)# session protocol {cisco sipv2}	Enters the session protocol type. The keywords are as follows: <ul style="list-style-type: none"> ■ cisco—Configures the dial peer to use proprietary CiscoVoIP session protocol. ■ sipv2—Configures the dial peer to use IETF SIP. SIP users should use this option.

Step	Command	Purpose
4.	<pre>Router(config-sip-ua)# sip- server {dns:[hostname] ipv4:ip_addr:[port-num]}</pre>	<p>Enters the host name or IP address of the SIP server interface. If you use this command, you can then specify session target SIP server for each dial peer instead of repeatedly entering the SIP server interface address for each dial peer. The keywords and arguments are as follows:</p> <ul style="list-style-type: none"> ■ <i>dns:hostname</i>: Sets the global SIP server interface to a domain name server (DNS) host name. A valid DNS host name takes the following format: <i>name.gateway.xyz</i>. ■ <i>ipv4:ip_addr</i>: Sets the IP address. ■ <i>portnum</i>: (Optional) Sets the UDP port number for the SIP server.
5.	<pre>Router(config-dial-peer)# session target {sip-server dns:[\$\$\$. \$d\$. \$e\$. \$u\$. [hostname] ipv4:ip_addr:[port-num]}</pre>	<p>Specifies a network-specific address for a dial peer. The keywords and arguments are as follows:</p> <ul style="list-style-type: none"> ■ <i>sip-server</i>: Sets the session target to the global SIP server. Used when the <i>sip-server</i> command has already specified the host name or IP address of the SIP server interface. ■ <i>dns:hostname</i>: Sets the global SIP server interface to a DNS host name. A valid DNS host name takes the following format: <i>name.gateway.xyz</i>. ■ <i>ipv4:ip_addr</i>: Sets the IP address. ■ <i>portnum</i>: (Optional) Sets the UDP port number for the SIP server. <p>Note: You can use wildcards when defining the session target for VoIP peers.</p>

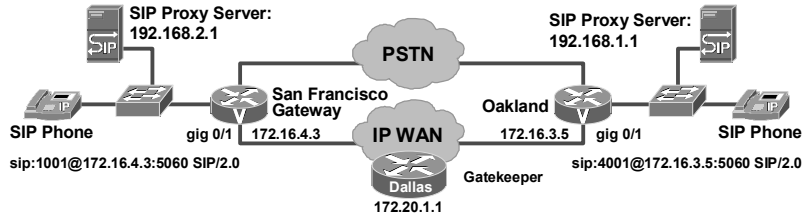
You do not need to configure a SIP user agent in order to place SIP calls. A SIP user agent is configured to listen for SIP traffic by default. However, if you want to adjust any of the SIP-related settings, use the following commands beginning in global configuration mode.

SIP-Related Settings

Step	Command	Purpose
1.	Router(config)# sip-ua	Enters the SIP user agent configuration mode to configure SIP user agent-related commands.
2.	Router(config-sip-ua)# transport {udp tcp}	Configures the SIP user agent for SIP signaling messages. The default is udp. The transport protocol (udp or tcp) specified with the session transport command must be identical to the protocol specified with the transport command.
3.	Router(config-sip-ua)# timers {trying <i>number</i> connect <i>number</i> disconnect <i>number</i> expires <i>number</i> }	(Optional) Configures the SIP signaling timers. The keywords are as follows: <ul style="list-style-type: none"> ■ trying: Sets the time to wait for a 100 response to an INVITE request. The default is 500. ■ connect: Sets the time to wait for a 200 response to an ACK request. The default is 500. ■ disconnect: Sets the time to wait for a 200 response to a BYE request. The default is 500. ■ expires: Limits the duration (in milliseconds) for which an INVITE is valid. The default is 180,000.
4.	Router(config-sip-ua)# retry {invite <i>number</i> response <i>number</i> bye <i>number</i> cancel <i>number</i> }	(Optional) Configures the SIP signaling timers for retry attempts. The keywords are as follows: <ul style="list-style-type: none"> ■ invite: Number of INVITE retries. The default is 6. ■ response: Number of RESPONSE retries. The default is 6. ■ bye: Number of BYE retries. The default is 10. ■ cancel: Number of CANCEL retries. The default is 10.
5.	Router(config-sip-ua)# max-forwards <i>number</i>	(Optional) Limits the number of proxy or redirect servers that can forward a request. The default is 6.
6.	Router(config-sip-ua)# max-redirects <i>number</i>	(Optional) Sets the maximum number of redirect servers. The default is 1.
7.	Router(config-sip-ua)# default {max-forwards retry {invite response bye cancel} sip-server timers {trying connect disconnect expires} transport}	(Optional) Resets the value of a SIP user agent command to its default.

SIP and H.323 Integration

Cisco.com



```
interface GigabitEthernet0/1
ip address 172.16.4.3 255.255.255.0
duplex full
speed 100
h323-gateway voip interface
h323-gateway voip id Dallas ipaddr 172.20.1.1 1719
h323-gateway voip h323-id SFGW
!
dial-peer voice 1 voip
application session
destination-pattern 4...
voice-class codec 1
voice-class h323 1
session protocol sipv2
session target ras
dtmf-relay h245-alphanumeric
```

```
interface GigabitEthernet0/1
ip address 172.16.3.5 255.255.255.0
duplex full
speed 100
h323-gateway voip interface
h323-gateway voip id Dallas ipaddr 172.20.1.1 1719
h323-gateway voip h323-id OAK
!
dial-peer voice 1 voip
application session
destination-pattern 1...
voice-class codec 1
voice-class h323 1
session protocol sipv2
session target ras
dtmf-relay h245-alphanumeric
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-18

If SIP is deployed in a network where H.323 is also used, there can be no performance limitations related to the call mix between SIP and H.323 calls, and there can be no significant deviation in calls-per-second measurements compared to a homogeneous SIP or H.323 network.

Gateways coordinate calls by communicating with gatekeepers using the Registration, Admission, and Status (RAS) protocol. Within a SIP network, an infrastructure proxy server controls call routing and performs functions such as registration, authentication, authorization, network access control, and network security. It finds the next-hop routing information based on received or translated destination URLs or E.164 addresses.

When both SIP and H.323 are deployed in a network, support of the two protocols on a single gateway is critical. Another integral part of dual-protocol deployment is the ability for H.323 gatekeepers and SIP proxies to interwork and share routing capabilities. The SIP proxy server actually acts like another gatekeeper to the H.323 network. This optimized routing structure provides a shorter post-dial delay and a more efficient use of gateway resources. It must be stressed that the SIP-proxy to gatekeeper communication is used only for call routing and not for any type of protocol translation.

This type of communication between SIP-based and H.323-based components also is used only for call signaling. SIP RTP streams only flow directly between SIP endpoints.

SIP Gateway Integration with Cisco CallManager

This topic describes how SIP gateways integrate with Cisco CallManager and Cisco CallManager Express in an IP telephony network.

Cisco CallManager 4.1(2) SIP Trunk Configuration

Cisco.com

Trunk Configuration

Product: SIP Trunk
Device Protocol: SIP
Status: Update completed.

Device Information

Device Name*	SIPTrunk
Description	CCMSIPTrk-to-ProxySrv
Device Pool*	Device_Pool_AB_HQ
Call Classification*	Use System Default
Media Resource Group List	<None>
Location	HQ
AAR Group	<None>
<input checked="" type="checkbox"/> Media Termination Point Required	
Destination Address*	172.16.3.1
<input type="checkbox"/> Destination Address is an SRV	
Destination Port	5060
Incoming Port*	5061
Outgoing Transport Type*	UDP
Preferred Originating Codec*	G711ulaw

1. Trunk
2. Route Group
3. Route List
4. Route Pattern
5. Test trunk

SCCP Phones

SIP Network

SIP Phones

Port Cisco CallManager uses to send SIP traffic to proxy server

Port Cisco CallManager listens to for incoming SIP traffic

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-1-19

In a call-processing environment that uses SIP, use SIP trunks to configure a signaling interface with Cisco CallManager for SIP calls. SIP trunks (or signaling interfaces) connect Cisco CallManager clusters with a SIP proxy server. A SIP signaling interface uses port-based routing, and Cisco CallManager accepts calls from any gateway as long as the SIP messages arrive on the port that is configured as a SIP signaling interface. The SIP signaling interface uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more endpoints.

Setting up the proxy server is beyond the scope of this course.

Cisco CallManager 4.1(2) SIP Trunk to SIP Trunk

1. Trunk
2. Route Group
3. Route List
4. Route Pattern
5. Test Trunk



Trunk Configuration

Product: SIP Trunk
Device Protocol: SIP
Status: Ready
[Update](#) [Delete](#) [Reset Trunk](#)

Device Information

Device Name*	SIPTrunkToCCMCluster2
Description	SIP_To_HQ
Device Pool*	DP_GW_CJ_IO
Call Classification*	Use System Default
Media Resource Group List	< None >
Location	HQ
AAR Group	< None >
<input checked="" type="checkbox"/> Media Termination Point Required	
Destination Address*	172.16.2.1
<input type="checkbox"/> Destination Address is an SRV	
Destination Port	5060
Incoming Port*	5061
Outgoing Transport Type*	UDP
Preferred Originating Codec*	G711ulaw

Trunk Configuration

Product: SIP Trunk
Device Protocol: SIP
Status: Ready
[Update](#) [Delete](#) [Reset Trunk](#)

Device Information

Device Name*	SIPTrunkToCCMCluster1
Description	SIP_To_HQ
Device Pool*	DP_SJC_HQ
Call Classification*	Use System Default
Media Resource Group List	< None >
Location	HQ
AAR Group	< None >
<input checked="" type="checkbox"/> Media Termination Point Required	
Destination Address*	172.16.1.1
<input type="checkbox"/> Destination Address is an SRV	
Destination Port	5061
Incoming Port*	5060
Outgoing Transport Type*	UDP
Preferred Originating Codec*	G711ulaw

Before deploying Cisco CallManager into a SIP environment, test the call flow between two CallManager clusters, if there are more than one cluster. This test will validate whether the CallManagers are configured correctly.

For more information, refer to the “Trunk Configuration” section in the “*Cisco CallManager Administration Guide*” at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book_09186a00802d8eaf.html.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- In configuring an H.323 gateway with Cisco CallManager, the first step is to set the H.225 timer to 3 seconds. The next step is to configure the dial peers.
- H.323 dial peers can be configured to define primary and backup Cisco CallManager servers with switchover to a backup server if necessary.
- In toll bypass situations, if the packet network bandwidth is constrained, or unavailable, the call is routed transparently to the PSTN gateway interface (dial peer #) for transport to the remote site.
- MGCP PRI backhaul terminates all of the ISDN PRI Layer 2 (Q.921) signaling functions on the MGCP gateway and packages all of the ISDN PRI Layer 3 (Q.931) signaling information into packets for transmission to Cisco CallManager through an IP tunnel.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-21

Summary (Cont.)

Cisco.com

- When both SIP and H.323 are deployed in a network, support of the two protocols on a single gateway is critical. Another integral part of dual-protocol deployment is the ability for H.323 gatekeepers and SIP proxies to interwork and share routing capabilities.
- In a call-processing environment that uses SIP, use SIP trunks to configure a signaling interface with Cisco CallManager for SIP calls. SIP trunks (or signaling interfaces) connect Cisco CallManager clusters with a SIP proxy server.
- When a Cisco CallManager Express router is deployed in SIP networks, its integration with SIP is via SIP gateway trunks for the support of basic calls.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-22

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) Why is it necessary to decrease the H.225 timer on the H.323 gateway to 3 seconds?
(Source: H.323 Gateway Integration with Cisco CallManager)

Q2) List the VoIP toll bypass types. (Source: H.323 Gateway Integration with Toll Bypass)

Q3) How can an H.323 voice gateway be configured to use redundant CallManagers?
(Source: H.323 Gateway Integration with Cisco CallManager)

- A) H.323 gateways can use the MGCP redundant host commands if they are configured. This configuration allows H.323 and MGCP to use the primary and backup Cisco CallManager.
- B) H.323 dial peers can be configured to define primary and backup CallManager servers with switchover to a backup server if necessary.
- C) Use the priority keyword when defining multiple IPV4 peers in the dial plan: always use 1 for the primary and 2 for the backup CallManager.
- D) Redundancy is configured on the CallManager where the intelligence lies, not on the gateway.

Q4) Where does MGCP PRI backhaul terminate all ISDN PRI Layer 2 (Q.921) signaling functions? (Source: MCGP Backhauling)

- A) MGCP PRI backhaul terminates all of the ISDN PRI Layer 2 (Q.921) signaling functions on the MGCP gateway.
- B) MGCP PRI backhaul terminates all of the ISDN PRI Layer 2 (Q.921) signaling functions on the Cisco CallManager.
- C) MGCP PRI backhaul cannot terminate ISDN PRI Layer 2 (Q.921) signaling; it can only terminate ISDN PRI Layer 3 (Q.931).
- D) MGCP PRI backhaul terminates all of the ISDN PRI Layer 2 (Q.921) signaling functions into QSIG packets for transmission to Cisco CallManager through an IP tunnel.

Q5) What information does MGCP PRI backhaul package for transmission to a CallManager? (Source: Source: MCGP Backhauling)

- A) all of the ISDN PRI Layer 2 (Q.921) signaling information
- B) all of the ISDN PRI Layer 3 (Q.931) signaling information
- C) just the display and user-to-user information elements
- D) just the tunneling of redirecting number information element

Q6) What are the key SIP and H.323 integration considerations? (Source: SIP Gateway Integration with Cisco CallManager)

Q7) What is required for a Cisco CallManager to make SIP calls? (Source: SIP Gateway Integration with CallManager)

Lesson Self-Check Answer Key

- Q1) This step is necessary because, by default, the H.225 timer that controls redirection to a less preferred dial peer on a “no-response” failure is considerably longer than the 10-second timer of the Q.931 Call Proceeding timer. By setting the H.225 timer to 3 seconds, the router attempts a connection to the primary Cisco CallManager server, and if it does not receive a response in 3 seconds, it falls back to the secondary Cisco CallManager server.
- Q2) Cisco CallManager to Cisco CallManager
Cisco CallManager to Cisco CallManager Express sites
Cisco CallManager to remote sites that are part of the same cluster
Cisco CallManager to remote sites under PBX control
PBX to other PBX-controlled sites
- Q3) B
- Q4) A
- Q5) B
- Q6) In deployments where both SIP and H.323 protocols are used, it is important that the calls-per-second performance of both environments is similar. Provisions for communication between the Cisco SIP proxy server and H.323 gatekeepers allow hybrid networks that include both SIP and H.323 traffic.
- Q7) Cisco CallManager requires an RFC 2833 DTMF-compliant MTP software device to make SIP calls. The current standard for SIP uses in-band payload types to indicate DTMF tones, and IP telephony components such as SCCP IP Phones only support out-of-band payload types. Thus, an RFC 2833-compliant MTP device monitors for payload type and acts as a translator between in-band and out-of-band payload types.

Lesson 4

Configuring Fax and Modem Support

Overview

Configuring fax and modem support on gateways is a complex task, and it remains one of the major challenges for network or system administrators because many organizations continue to use analog fax machines that use complicated tone-based protocols to establish connections and pass on information. This lesson discusses fax relay, fax pass-through, modem relay, and modem pass-through solutions. It also discusses best practices for the configuration of modem and fax as voice in VoIP.

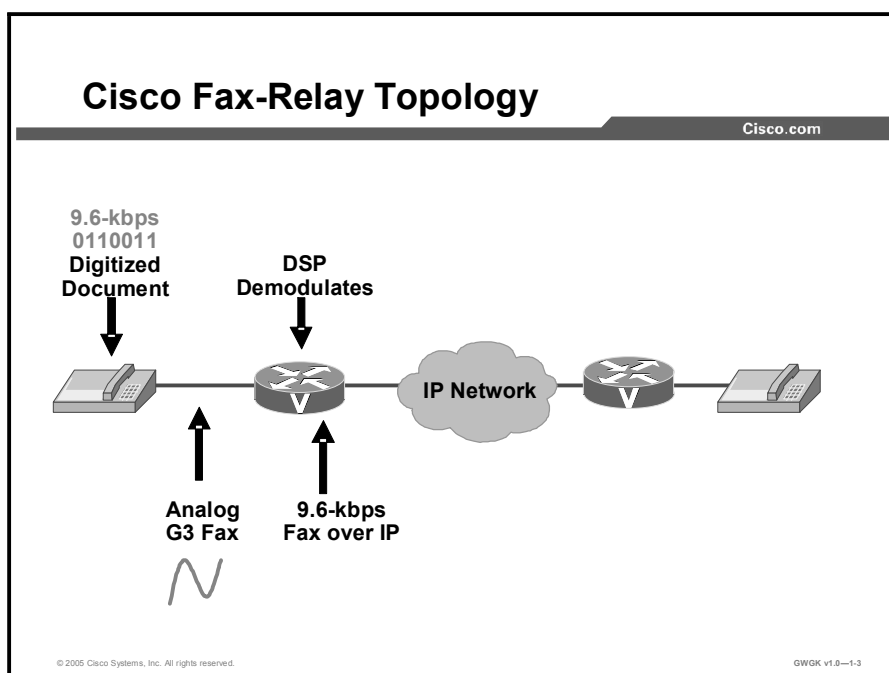
Objectives

Upon completing this lesson, you will be able to explain how fax and modem traffic are supported on an H.323, an MGCP, and a SIP gateway. This ability includes being able to meet these objectives:

- Explain the fax relay solution
- Explain the fax pass-through solution
- Describe the best practices for configuring fax as voice in VoIP
- Explain the modem relay solution
- Explain the modem pass-through solution
- Describe the best practices for configuring modem as voice in VoIP

Fax Relay

The topic explains the fax-relay solution to the problem of fax as voice in a VoIP environment.



Fax relay is a technique used to overcome the deficiency in high compression voice codecs, such as G729 or G723, when these codecs try to pass fax traffic.

Since a fax call is treated like a regular speech call, the digital signal processor (DSP) in each gateway goes into voice mode. After this conversion, the DSP expects to receive and process human speech. During the life of the call, if the DSP hears a fax answer, caller-entered digits (CEDs), or calling tone, the DSP does not interfere with the speech processing. Instead, the DSP allows the tone to continue across the VoIP call leg.

After generating a CED or hearing a calling tone, a fax machine transmits a T.30 digital information signal (DIS) message as part of fax handshaking. This process usually occurs at the terminating fax machine. The terminating gateway DSP then detects the High-Level Data Link Control (HDLC) flag sequence at the start of the DIS message and initiates fax relay switchover. The terminating gateway unloads the voice codec and loads a fax codec to handle the fax call.

Notification also is sent to the DSP on the other side of the VoIP network so that the DSPs on each side of the fax call are using the fax codec. The notification mechanisms differ depending on the fax relay protocol used. With the fax codec loaded, the DSPs demodulate the T.30 HDLC frames, extract the fax information, and pass it between the routers using one of the following fax relay protocols:

- **Proprietary Cisco fax relay for VoIP:** Fax relay is the default mode for passing faxes through a VoIP network and Cisco fax relay is the default fax-relay type. This capability has been supported in Cisco IOS Releases 11.3 and later, is widely available, and uses Real-Time Transport Protocol (RTP) to transport the fax data.

- **Standards-based T.38 fax for VoIP:** T.38 has been available in Cisco IOS Software Releases 12.1(3)T and later on some platforms. You can enable it with the fax relay protocol **t38** command configured under the VoIP dial peer. It uses User Data Protocol (UDP) to transport fax data.
- **Standards-based FRF.11 Annex D for Voice over Frame Relay (VoFR) and Voice over Asynchronous Transfer Mode (VoATM).**

It is important to understand that unlike in-band faxing or fax pass-through, fax relay breaks down the T.30 fax tones into their specific HDLC frames (demodulation), transmits the information across the VoIP network using the fax-relay protocol, and then converts the bits back into tones at the far side (modulation). The fax machines on either end are sending and receiving tones and are not aware that a demodulation and modulation fax-relay process is occurring.

Cisco fax relay and T.38 fax relay also differ from T.37 fax store and forward. T.37 provides a standards-based method of allowing a VoIP gateway to receive the following:

- A fax from a fax machine and forward it to an SMTP-capable mail server, which can then deliver the fax to a user as an e-mail message
- An e-mail message from a mail server and modulate it into a fax signal for receipt by a regular fax machine

Fax-Relay Optimization Commands

Cisco.com

```
C1C1GW(config-dial-peer)#
```

```
fax rate {2400|4800|7200|9600|12000|14400|disable|voice}
```

- **Example:** fax rate 9600 voice

```
C1C1GW(config-dial-peer)#
```

```
fax-relay ecm disable
```

- **Disables fax-relay ECM**

```
C1C1GW(config-dial-peer)#
```

```
fax NSF word
```

- **word indicates country and manufacturer**

```
C1C1GW(config-dial-peer)#
```

```
fax protocol {cisco|none|system|pass-through  
{g711ulaw|g711alaw}}
```

- **Disables fax-relay ECM**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1.4

Fax relay exists, by default, on VoIP platforms. If voice calls complete successfully between two routers, fax calls should also work. However, when fax relay does not work or performance needs to be improved, there are some fax-relay-specific commands you can issue as a precursor to troubleshooting the problem.

The **fax rate** command is configured under the VoIP dial peer in configuration mode. The default setting is fax rate **voice**, which does not appear in the configuration under each dial peer.

The fax rate voice setting restricts the fax rate to the codec bandwidth. This restriction means that if the dial peer is configured to use the default G.729 voice codec that compresses voice to 8 kbps, the fax rate voice setting would not allow fax calls to exceed this codec bandwidth. The fax would be limited to a bandwidth of 7200 bits per second (bps), even if it tried initially to negotiate at a higher bandwidth of 14,400 bps or 9600 bps.

A common complaint is that faxes that used to complete within a certain time when the fax machine was connected via the public switched telephone network (PSTN) now take twice as long to complete. This behavior is expected if a low-bandwidth codec such as G.729 has been configured with the default fax rate voice setting. Using the **fax rate** command, you can configure fax transmissions to use a bandwidth greater than the codec compression. The command **fax rate 14400** allows fax calls to negotiate to a maximum of 14,400 bps regardless of the voice codec that is configured. This configuration resolves the problem of longer completion times.

However, the main purpose of the **fax rate** command within voice networks is to determine bandwidth use per call. The fax rate voice setting is the default because it ensures that both voice and fax calls use the same amount of bandwidth within the network. You should consider these factors when you are changing the fax rate to something greater than that of the codec bandwidth.

Note Some fax machines may operate more stably at a rate different from the default. In this case, the **fax rate** command can be used to test operation at different speeds.

The **fax-relay ECM disable** command is available for Cisco fax relay only and is issued to disable Error Correction Mode (ECM) negotiation between a pair of fax machines. ECM ensures that the faxed pages are transmitted error free and is a feature that is usually found on higher-end fax machines. Unfortunately, ECM has a low tolerance (approximately two percent) for jitter and packet loss. Therefore, when this negotiated feature is enabled, it may result in a higher fax-failure rate in VoIP networks. Incomplete output on the terminating fax is a symptom of failures caused by packet loss.

If both fax machines agree during the fax negotiation phase, ECM is enabled. However, during fax relay, the routers demodulate the fax tones into their true HDLC frame format. As a result, the routers are able to intercept and overwrite the field in the frame that indicates ECM status. If a fax machine transmits ECM capability, the router can change this parameter so that the other fax machine believes that ECM is not supported. Both fax machines are then forced to disable ECM, which results in using standard T.4 data to transmit the fax data.

Fax reliability is increased greatly with ECM disabled, even with much higher packet loss (about 10 percent) and delay. In addition, the **fax-relay ECM disable** command automatically enables a Cisco IOS software feature called “packet loss concealment” whereby lost scan lines are repeated to spoof the receiving fax machine into believing that it is receiving all the data.

Note While ECM may improve the success rate of fax transmissions in badly configured voice networks, the underlying network problems remain and should be addressed to prevent other problems from occurring.

Disabling ECM is a straightforward configuration step that you perform under the VoIP dial peer. As noted in the command reference, this command currently works only for VoIP dial peers.

The **fax NSF** command is used to prevent the transfer of proprietary fax capabilities. Since the router fax relay implementation demodulates and decodes the fax tones based on the T.30 specification, proprietary transactions or encoding break fax relay and cause the fax transmission to fail. Certain brands of fax machines use these proprietary encodings to signal the availability of enhanced capabilities, which help a fax manufacturer distinguish its products from others. This capability notification takes place using the optional Non Standard Facilities (NSF) field during fax negotiation.

When you issue the **fax NSF** command, the router overwrites the NSF so only standard fax transactions will occur. Vendor-specific facilities that are beyond the standard Group 3 requirements, and that break Cisco fax relay, are prevented from being used. When this command is issued, the NSF is set to all zeros, and this should fix problems caused by the NSF field.

The **fax protocol** command is required for VoIP to specify which fax-relay protocol (T.38 or Cisco fax relay) will be used.

The *cisco* option configures Cisco fax relay. The *t38* option disables Cisco fax relay and enables T.38. Certain voice platforms support only T.38. Hence, for interoperability, you must explicitly configure T.38 on platforms where Cisco fax relay is the default. The *system* option allows the dial peer to inherit the fax relay protocol that is configured globally with the **voice service voip** command. If nothing is configured under the **voice service voip** command, the default is Cisco fax relay.

The default setting of the **fax protocol** command is the system option. Because the system option defaults to Cisco fax relay, VoIP dial peers always default to Cisco fax relay when no protocol has been explicitly configured.

Configuring Cisco Fax-Relay Support

Cisco.com

Individual VoIP Dial Peers

```
1. dial-peer voice tag voip
2. fax protocol {cisco | none | system | pass-through
   {g711ulaw | g711alaw}}
3. fax rate {12000 | 14400 | 2400 | 4800 | 7200 | 9600 |
   disable | voice} [bytes rate]
4. fax-relay ecm disable
5. fax nsf word
6. exit
```

VoIP Dial Peers Globally

```
1. voice service voip
2. fax protocol {cisco | none}
3. exit
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1.5

On platforms that support it, Cisco fax relay is enabled by default. However, there are also two commands that allow you explicitly to select Cisco fax relay, either for an individual dial peer or globally for all dial peers. Several other commands allow you to set various fax parameters. Fax relay parameters that are set for an individual dial peer under the **dial-peer voice** command take precedence over global settings made under the **voice service voip** command. Cisco fax relay uses RTP to transport the fax data. Cisco fax relay is configured on the VoIP dial peers that direct calls into and out of the packet network.

Note Some Cisco platforms such as the Cisco AS5350 Universal Gateway, Cisco AS5400 Series Universal Gateways, Cisco AS5800 Series Universal Gateway, and Cisco AS5850 Universal Gateway do not support Cisco fax relay.

To configure one or more individual VoIP dial peers, use the following commands: (This task allows you to specify Cisco fax-relay parameter values for individual dial peers.)

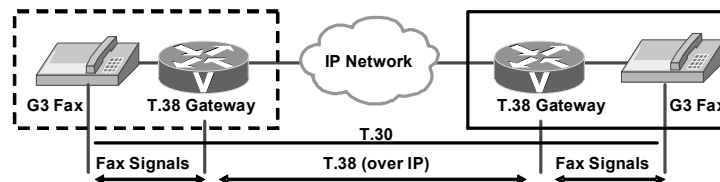
- **dial-peer voice tag voip**
- **fax protocol {cisco | none | system | passthrough {g711ulaw | g711alaw}}**
- **fax rate {12000 | 14400 | 2400 | 4800 | 7200 | 9600 | disable | voice} [bytes rate]**
- **fax-relay ecm disable**
- **fax nsf word**
- **exit**

To configure VoIP dial peers globally, complete the following steps:

- Step 1** Enter **voice service voip**.
- Step 2** Enter **fax protocol{cisco|none}**.
- Step 3** Enter **exit**.

T.38 Topology

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-6

The T.38 fax relay for VoIP H.323 feature provides standards-based fax-relay protocol support. The Cisco fax-relay solution is not always an ideal solution for enterprise and service provider customers who have a mixed vendor network. Because the T.38 fax relay protocol is standards-based, Cisco gateways and gatekeepers are able to interoperate with third-party T.38-enabled gateways and gatekeepers in a mixed vendor network where real-time fax-relay capabilities are required.

The figure shows a T.38 topology. G3 fax machines are attached at either end of an IP network. Fax signals are sent between a G3 fax machine and a T.38 gateway. T.38 gateways translate fax signals into IP packets, and then send them over an IP network using the T.38 protocol. T.30 is used to support fax transmission across the network. For example, when a fax is sent from the originating gateway, an initial voice call is established. The terminating gateway detects the fax tone that was generated by the answering fax machine. The VoIP H.323 call stack then starts a T.38 mode request using H.245 procedures. If the opposite end of the call acknowledges the T.38 mode request, the initial audio channel is closed and a T.38 fax relay channel is opened. When the fax transmission is completed, the call is reverted back to voice mode.

Note Some Cisco voice gateways do not currently support T.38. Because of the restricted availability of T.38 support on the voice gateways, detailed information about it is beyond the scope of this lesson. Briefly, you need to configure T.38 fax relay in both the originating and terminating H.323 gateways for the T.38 fax relay for VoIP to operate.

Only UDP is implemented for T.38 fax relay for VoIP H.323 gateway support on the multiservice gateways for the Cisco IOS Software Release 12.1(3)T. Transmission Control Protocol (TCP) T.38 fax relay is not supported.

Note TCP and UDP are the transport protocols that are specified in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendation for T.38. However, only UDP is supported for Cisco IOS Software Release 12.1(3)T. For further information on T.38 protocol, refer to the ITU-T T.38 recommendation.

You must complete voice interoperability testing with third-party gateways and gatekeepers before configuring the T.38 fax relay for the VoIP H.323 feature in your network because different companies may select certain parts of H.323 and T.38 to implement into their gateways and gatekeepers. The following are T.38 fax-relay requirements:

- T.38 fax-relay interoperability requires H.323 version 2.
- T.38 fax relay is not supported by Multimedia Conference Manager (MCM) H.323 proxy in Cisco IOS Software Release 12.1(3)T.
- T.38 fax relay is not supported in conjunction with Media Gateway Control Protocol (MGCP), Simple Gateway Control Protocol (SGCP), or Session Initiation Protocol (SIP) in Cisco IOS Software Release 12.1(3)T.

For additional information about implementing T.38 on these Cisco voice gateways, see the “T.38 fax relay for Voice over IP H.323” feature in the *Cisco IOS Voice Command Reference, Release 12.3* at

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a00801e8a79.html.

Also, see the “Platform Support for Cisco Fax Services” section in the *Cisco Fax Services over IP Application* available at

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide_chapter09186a00800b5dce.html#wp1158490.

Prerequisites for T.38 Fax Relay for VoIP

Cisco.com

Check for the following:

- A Cisco IOS software release that supports fax pass-through is running.
- There is a working VoIP H.323 or SIP network for voice calls.
- There has been complete voice interoperability testing with third-party gateways and gatekeepers.
- There is a minimum of 64 MB of RAM.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1.7

Ensure that the following have been performed or checked before configuring VoIP H.323 for the T.38 fax relay:

- Cisco IOS Software Release 12.1(3)T is running on the Cisco AS5300 Series Universal Access Server.
- There is a working VoIP H.323 network for voice calls.
- Voice interoperability testing with third-party gateways and gatekeepers has been completed.
- There is a minimum of 64 MB of RAM.

Note Although 96 to 128 MB of RAM is recommended, the memory requirement depends on the platform and the anticipated number of calls to be made through the system.

Configuring T.38 Fax Relay for VoIP H.323 Globally (Required)

Cisco.com

	Command
Step 1	Router(config)# voice service voip
Step 2	Router(config-voi-serv)# fax protocol {cisco t38 [ls_redundancy value] [hs_redundancy value]}
Step 3	Router(config-voi-serv)# exit
Step 4	Router(config)# exit

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1.8

You need to configure T.38 fax relay in both the originating and terminating gateways for the T.38 fax relay for VoIP H.323 to operate. To specify the global default fax protocol for all the VoIP dial peers, configure the dial peers in global configuration mode. To specify the fax protocol for a specific VoIP dial peer, configure the dial peer in dial-peer configuration mode.

Fax relay parameters that are set for an individual dial peer under the **dial-peer voice** command take precedence over global settings made under the **voice service voip** command.

To configure T.38 fax relay for VoIP H.323 for all the connections of a gateway, use the commands provided in the “Configure T.38 Fax Relay for VoIP H.323 Globally” table and be sure to begin in global configuration mode. (Repeat the configuration steps on both the originating and terminating gateways.)

Configure T.38 Fax Relay for VoIP H.323 Globally

Step	Command	Description
1.	Router(config)# voice service voip	Enters the voice-service configuration mode.
2.	Router(config-voi-serv)# fax protocol {cisco t38 [ls_redundancy value] [hs_redundancy value]}	<p>This command specifies the global default fax protocol for all the VoIP dial peers. The t38 keyword enables the T.38 fax relay protocol. The cisco keyword selects the original Cisco proprietary fax protocol. Optional parameters ls_redundancy and hs_redundancy are used to send redundant T.38 fax packets.</p> <p>Note: The ls_redundancy and hs_redundancy parameters are applicable only to the T.38 fax relay protocol.</p> <p>The ls_redundancy parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol. For the ls_redundancy parameter, the <i>value</i> can be from 0 to 5. The default is 0 (no redundancy). The parameter <i>value</i> sets the redundancy factor for the T.38 fax relay.</p> <p>The hs_redundancy parameter refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. For the hs_redundancy parameter, the <i>value</i> can be from 0 to 2. The default is 0 (no redundancy). The parameter <i>value</i> sets the redundancy factor for the T.38 fax relay.</p> <p>Note: Setting the hs_redundancy parameter to greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.</p>
3.	Router(config-voi-serv)# exit	Exits the voice-service configuration mode and returns to the global configuration mode.
4.	Router(config)# exit	Exits the global configuration mode.

Configuring T.38 Fax Relay for a Specific Dial Peer (Optional)

Cisco.com

	Command
Step 1	<code>Router(config)# dial-peer voice tag voip</code>
Step 2	<code>Router(config-dial-peer)# fax protocol {cisco t38 [ls_redundancy value] [hs_redundancy value] system}</code>
Step 3	<code>Router(config-dial-peer)# fax rate {12000 14400 2400 4800 7200 9600} {disable voice} [bytes rate]</code>

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1.9

When T.38 fax relay is configured under the dial-peer voice configuration, the configuration for the specific dial peer takes precedence over the global configuration under the **voice service voip** command.

To configure T.38 fax relay for VoIP H.323 for a specific dial peer, use the following commands provided in the “Configure T.38 Fax Relay for VoIP H.323 for a Specific Dial Peer” table and begin in dial-peer configuration mode. Repeat the configuration steps on both the originating and terminating gateways.

Configure T.38 Fax Relay for VoIP H.323 for a Specific Dial Peer

Step	Command	Description
1.	Router(config)# dial-peer voice tag voip	Enters dial-peer configuration mode.
2.	Router(config-dial-peer)# fax protocol {cisco t38 [ls_redundancy value] [hs_redundancy value] system}	<p>This command specifies the fax protocol for a dial peer. The t38 keyword enables the T.38 fax relay protocol. The cisco keyword selects the original Cisco proprietary fax protocol. When the system keyword is selected in the dial peer, it specifies the global default fax protocol used by a dial peer, set by the fax protocol t.38 command. Optional parameters ls_redundancy and hs_redundancy are used to send redundant T.38 fax packets.</p> <p>Note: The ls_redundancy and hs_redundancy parameters are applicable only to the T.38 fax relay protocol.</p> <p>The ls_redundancy parameter refers to data redundancy in the low-speed V.21-based T.30 fax machine protocol. For the ls_redundancy parameter, the <i>value</i> can be from 0 to 5. The default is 0 (no redundancy). The parameter <i>value</i> sets the redundancy factor for the T.38 fax relay.</p> <p>The hs_redundancy parameter refers to data redundancy in the high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. For the hs_redundancy parameter, the <i>value</i> can be from 0 to 2. The default is 0 (no redundancy). The parameter <i>value</i> sets the redundancy factor for the T.38 fax relay.</p> <p>Note: Setting the hs_redundancy parameter to greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.</p>
3.	Router(config-dial-peer)# fax rate {12000 14400 2400 4800 7200 9600} {disable voice} [bytes rate]	Selects the maximum fax transmission speed for a dial peer.

Example: T.38 Fax Relay for VoIP H.323 Configuration

Cisco.com

```
Router# show running-config
Building configuration...
Current configuration:
. . . . .
voice service voip
fax protocol t38
. . . . .
interface Ethernet0/0
ip address 10.0.47.47 255.255.0.0
h323-gateway voip interface
h323-gateway voip id ipaddr
10.0.47.36 1719
h323-gateway voip h323-id 36402
. . . . .
```

```
dial-peer voice 14151 voip
!!! Uses t38 fax from voice
service voip
destination-pattern 14151..
session target ras
!
dial-peer voice 14152 voip
!!! Uses Cisco fax for a
specific dialpeer
destination-pattern 14152..
session target ras
fax protocol cisco
!
gateway
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-10

As discussed previously, T.38 fax relay is real-time fax transmission where two fax machines communicate with each other as if there were a direct phone line between the two.

Cisco provides two methods for fax relay: A proprietary Cisco method and a method based on the ITU-T T.38 standard. On most platforms, Cisco fax relay is the default if a fax method is not explicitly configured. On the left of the screen capture in the figure, the command enables the T.38 fax relay feature. Fax relay is configured using a few additional commands on gateway dial peers that have already been defined and configured for voice calls. On the right of the screen capture, the highlighted comments declare the type of T.38 configuration enabled: T.38 fax from the **voice service voip** command in the first and Cisco fax for a specific dial peer in the second configuration.

For additional information on Cisco fax relay, see the “Configuring Cisco Fax Relay” chapter in *Cisco IOS Fax Services over IP Configuration Guide Release 12.3(1)* at http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide_book09186a008017cf32.html.

T.37 Store-and-Forward Fax

Cisco.com

Two modes of operation

- **On-ramp: Receives faxes that are delivered as e-mail attachments**
- **Off-ramp: Sends standard e-mail messages that are delivered as faxes**

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0—1.11

T.37 store-and-forward fax consists of these two processes:

- **On-ramp faxing**, in which a voice gateway that handles incoming calls from a standard fax machine or the PSTN converts a traditional Group 3 fax into an e-mail message with a Tagged Image File Format (TIFF) attachment. An e-mail server handles the fax e-mail message and attachment while they are traversing the packet network, and they can be stored for later delivery or delivered immediately to a PC or to an off-ramp gateway.
- **Off-ramp faxing**, in which a voice gateway that handles calls going out from the network to a fax machine or the PSTN converts a fax e-mail with a TIFF attachment into a traditional fax format that can be delivered to a standard fax machine or to the PSTN.

On-ramp and off-ramp faxing processes can be combined on a single gateway, or they can occur on separate gateways. Store-and-forward fax uses two different interactive voice response (IVR) applications for on-ramp and off-ramp functionality. The applications are implemented in two Tool Command Language (TCL) scripts that you can download from Cisco.com.

Simple Mail Transfer Protocol (SMTP) facilitates the basic functionality of store-and-forward fax and has additional functionality that provides confirmation of delivery by using existing SMTP mechanisms, such as Extended Simple Mail Transfer Protocol (ESMTP).

Store-and-forward fax requires you to configure gateway dial peers and to specify values for the following types of parameters:

- **IVR application parameters and IVR security and accounting parameters:** These items load the applications on the router and also enable authorization and accounting for the application.
- **Fax parameters:** These items specify the cover sheet and header information that appears on faxes that are generated in the packet network.
- **Mail Transfer Agent (MTA) parameters:** These items define delivery parameters for the e-mail messages that accompany fax TIFF images.

- **Message disposition notification (MDN) parameters:** These items specify the generation of messages to notify e-mail originators when their fax e-mail messages have been delivered.
- **Delivery status notification (DSN) parameters:** These items instruct the SMTP server to send messages to e-mail originators to inform them of the status of their e-mail messages.
- **Gateway security and accounting parameters:** These items define authentication, authorization, and accounting (AAA) for faxes that enter or exit the packet network.

Note Store-and-forward fax configuration tasks are the same for H.323 and SIP networks. MGCP networks are not supported for store-and-forward fax capabilities.

Fax calls from the PSTN enter the network through an on-ramp gateway, which is sometimes called an originating gateway. Fax calls exit the packet network to the PSTN through an off-ramp gateway, which is sometimes called a terminating gateway. In small networks, on-ramp and off-ramp functionality can reside in the same gateway. For store-and-forward fax, each type of gateway is configured for the following two types of dial peers:

- The on-ramp gateway is configured with one or more plain old telephone service (POTS) dial peers to handle fax calls inbound to the gateway from the PSTN and with one or more Multimedia Mail over IP (MMoIP) dial peers to direct calls outbound from the gateway to the network.
- The off-ramp gateway is configured with one or more MMoIP dial peers to handle fax calls inbound from the IP network and with one or more POTS dial peers to direct calls outbound through POTS voice ports to the PSTN.

Note The instructions in this lesson assume that your packet network includes separate gateways for on-ramp and off-ramp functions. For smaller networks that use a single router for both on-ramp and off-ramp functionality, follow both the on-ramp and off-ramp instructions on the same router.

On-Ramp Gateway Configuration for T.37 Fax

Cisco.com

	Description
Step 1	Enabling T.37 store-and-forward fax on the on-ramp gateway (required)
Step 2	Configuring dial peers on the on-ramp gateway (required)
Step 3	Configuring MTA parameters on the on-ramp gateway (required)
Step 4	Configuring DSNs on the on-ramp gateway (optional)
Step 5	Configuring security and accounting on the on-ramp gateway (optional)
Step 6	Configuring T.37 IVR application security and accounting (optional)

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0—1-12

The configuration of T.37 store-and-forward fax is a detailed process and is beyond the scope of this course. However, the steps for configuration are outlined in the “On-Ramp Gateway Configuration for Store-and-Forward Fax” table, and the complete process can be reviewed in the *Cisco Fax Services over IP Application Guide*, which can be found at http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide_chapter09186a00800b5def.html#wp1083029.

On-Ramp Gateway Configuration for Store-and-Forward Fax

Step	Action	Notes
1.	<p>To enable T.37 store-and-forward fax on the on-ramp gateway (required), use the following commands:</p> <ul style="list-style-type: none"> ■ <code>ip domain-name name</code> ■ <code>call application voice application-name location</code> ■ <code>fax interface-type {fax-mail modem}</code> ■ <code>fax send transmitting-subscriber {\$s\$ string}</code> 	<p>The purpose of this task is to enable T.37 store-and-forward fax by specifying the following information:</p> <ul style="list-style-type: none"> ■ A fully qualified domain name for the SMTP server ■ Name and location of the T.37 application ■ Type of T.37 processing to occur on this gateway ■ Called-subscriber number definition
2.	<p>To configure dial peers on the on-ramp gateway, (required) use the following commands:</p> <ul style="list-style-type: none"> ■ <code>dial-peer voice tag pots</code> ■ <code>application application-name</code> ■ <code>direct-inward-dial</code> ■ <code>incoming called-number string</code> ■ <code>exit</code> 	<p>The purpose for configuring on-ramp gateway dial peers is to allow the router to receive inbound fax traffic from the PSTN and to direct the traffic to the appropriate SMTP server.</p>
3.	<p>To configure MTA parameters on the on-ramp gateway (required), use the following commands:</p> <ul style="list-style-type: none"> ■ <code>mta send server {host-name ip-address [port port-number]}</code> ■ <code>mta send postmaster e-mail-address</code> ■ <code>mta send mail-from hostname string</code> ■ <code>mta send mail-from username {string \$s\$}</code> ■ <code>mta send subject string</code> ■ <code>mta send origin-prefix string</code> ■ <code>mta send return-receipt-to {hostname string username string username \$s\$}</code> 	<p>The on-ramp gateway uses the sending Message Transfer Agent (MTA) and dial peers to receive fax calls from the PSTN and to define delivery parameters for the resulting e-mail message with the attached fax TIFF file. The purpose of this task is to configure parameter values associated with the MTA on the on-ramp gateway.</p>
4.	<p>Configure DSNs on the on-ramp gateway (optional).</p>	<p>The <code>dsn</code> command allows you to enable or disable the generation of DSNs for each state by reissuing the command and specifying a different notification option each time.</p>
5.	<p>Configure security and accounting on the on-ramp gateway (optional).</p>	<p>This is an optional step.</p>
6.	<p>Configure T.37 IVR application security and accounting (optional).</p>	<p>This is an optional step.</p>

Off-Ramp Gateway Configuration for T.37 Fax

Cisco.com

	Description
Step 1	Enabling T.37 store-and-forward fax on the off-ramp gateway (required)
Step 2	Configuring dial peers on the off-ramp gateway (required)
Step 3	Configuring fax headers and cover pages on the off-ramp gateway (optional)
Step 4	Configuring MTA parameters on the off-ramp gateway (required)
Step 5	Configuring MDNs on the off-ramp gateway (optional)
Step 6	Configuring security and accounting on the off-ramp gateway (optional)
Step 7	Configuring T.37 IVR application security and accounting on the off-ramp gateway (optional)

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-13

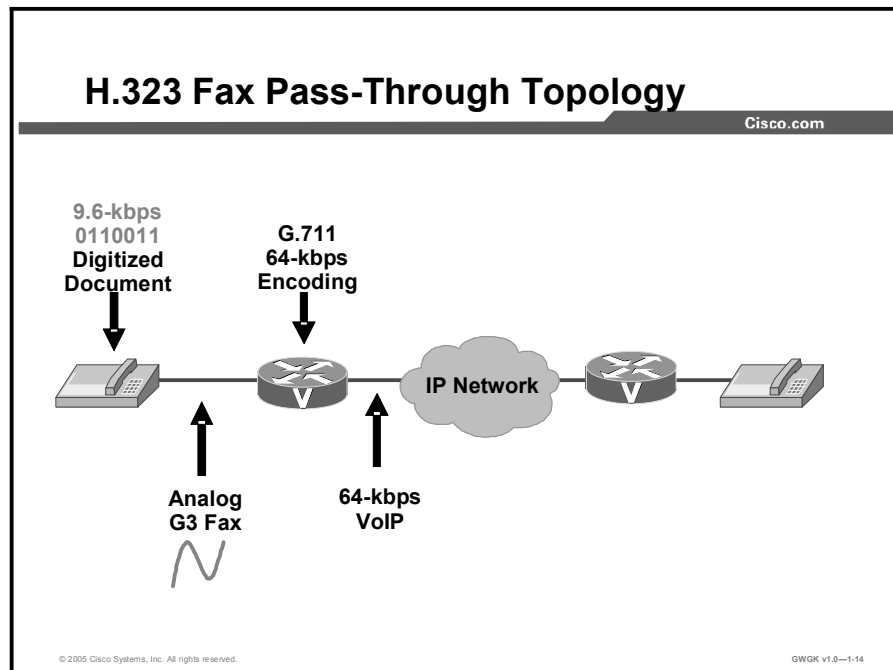
The steps for configuring off-ramp gateway configuration for T.37 are outlined in the “Off-Ramp Gateway Configuration for Store-and-Forward Fax” table.

Off-Ramp Gateway Configuration for Store-and-Forward Fax

Step	Action	Notes
1.	To enable T.37 store-and-forward fax on the off-ramp gateway (required), use the following commands: <ul style="list-style-type: none"> ■ <code>ip domain-name name</code> ■ <code>call application voice application-name location</code> ■ <code>fax interface-type {fax-mail modem}</code> ■ <code>fax send transmitting-subscriber {\$s\$ string}</code> 	The purpose of this task is to enable T.37 store-and-forward fax by specifying the following information: <ul style="list-style-type: none"> ■ A fully qualified domain name for the SMTP server ■ The name and location of the T.37 application ■ The type of T.37 processing to occur on this gateway ■ Transmitting-subscriber number definition
2.	To configure dial peers on the off-ramp gateway (required), use the following commands: <ul style="list-style-type: none"> ■ <code>dial-peer voice tag mmoip</code> ■ <code>application application-name</code> ■ <code>incoming called-number string</code> ■ <code>information-type fax</code> ■ <code>image encoding {mh mr mmr passthrough}</code> ■ <code>image resolution {fine standard super-fine passthrough}</code> ■ <code>exit</code> 	The purpose for configuring off-ramp gateway dial peers is to allow the router to receive inbound fax traffic from an SMTP server in the packet network and to direct that traffic to voice ports that interface with the PSTN.
3.	Configure fax headers and cover pages on the off-ramp gateway (optional).	The purpose of this task is to create headers and cover pages for fax messages that originate from plain-text e-mail messages. This task does not apply to fax TIFF files because headers and cover pages are generated by the originating fax machines and because the off-ramp gateway does not alter TIFF files when converting them.
4.	To configure MTA parameters on the off-ramp gateway (required), use the following commands: <ul style="list-style-type: none"> ■ <code>mta receive aliases string</code> ■ <code>mta receive maximum-recipients number</code> ■ <code>mta receive generate</code> 	The purpose of this task is to configure the way in which the off-ramp gateway receives messages from the MTA.
5.	Configure MDNs on the off-ramp gateway (optional).	This is an optional step.
6.	Configure security and accounting on the off-ramp gateway (optional).	This is an optional step.
7.	Configure T.37 IVR application security and accounting on the off-ramp gateway (optional).	This is an optional step.

Fax Pass-Through

The topic explains the fax pass-through solution to the problem of fax as voice in a VoIP environment.



Fax pass-through occurs when incoming fax data is not demodulated or compressed for its transit through the packet network. In the figure, the two fax machines communicate directly with each other over a transparent IP connection.

Note In this lesson, the terms fax pass-through and modem pass-through are used. The *Cisco IOS Voice Command Reference, Release 12.3 T* uses these commands in this way and that practice is followed in this lesson.

When a gateway in fax pass-through mode detects a fax tone, it switches the call to a high-bandwidth codec. The fax traffic, still in pulse code modulation (PCM) form, travels in-band over VoIP using G.711 and no voice activity detection (VAD). This method of transporting fax traffic takes a constant 64 kbps (payload) stream end to end for the duration of the call. Call Admission Control (CAC) must be engineered to provide adequate bandwidth for expected peak fax traffic and also voice traffic using G.729 compression. Fax pass-through is susceptible to packet loss, jitter, and latency in the IP network, even though packet redundancy can be used to mitigate the effects of packet loss.

Fax pass-through is supported under the following call control protocols:

- H.323
- SIP
- MGCP
- Fax pass-through signaling using the protocol stack or Named Signaling Events (NSEs)

When a fax tone is detected, the originating and terminating gateways need to communicate to each other that they are changing to fax pass-through mode. Gateway signaling of the changeover to fax mode can use either of these methods:

- H.323 or SIP protocol stack (fax pass-through)
- NSEs (modem pass-through)

New with Cisco IOS Software Release 12.2(13)T is the ability to specify the use of the H.323 or SIP protocol stack to signal the changeover to fax mode. This is enabled with the **fax protocol pass-through** command.

Alternatively, you can use the **modem passthrough** command to configure the gateway to use proprietary Cisco NSEs to signal the switch to pass-through mode. Pass-through using NSEs has been available on the Cisco AS5300 Series Universal Gateway since Cisco IOS Software Release 12.1(3)T and on most other platforms since Cisco IOS Software Release 12.2(11)T.

Modem pass-through is preferred if all of the involved gateways are Cisco IOS gateways. If other gateways are involved in the fax transmissions, fax pass-through must be used. In all cases, however, T.38 fax relay is the best solution if all of the involved gateways support it.

H.323 or SIP Support of Resource Reservation Protocol

As of Cisco IOS Software Release 12.2(13)T, H.323 or SIP gateways that are configured for fax pass-through or modem pass-through allow Resource Reservation Protocol (RSVP) bandwidth adjustments when the original voice call is configured to use RSVP. When the original voice codec is restored at the end of the fax session, the original RSVP bandwidth is restored as well. When current bandwidth is unavailable, the fax proceeds at a best-effort rate without RSVP and with no performance guarantees. RSVP bandwidth adjustments for fax transmissions are made as follows:

- **T.38 fax relay:** RSVP bandwidth is adjusted to 80 kbps.
- **Fax passthrough:** RSVP bandwidth is adjusted to 96 kbps.

H.323 Support for CAC

As of Cisco IOS Software Release 12.2(13)T, H.323 CAC adjustments are allowed in the case of fax pass-through and modem pass-through. An H.323 gateway that uses a gatekeeper requests the following bandwidths from the gatekeeper when codec changes are necessary:

- **T.38 fax relay:** Bandwidth of 80 kbps
- **Fax passthrough:** Bandwidth of 96 kbps

If the gatekeeper accepts the bandwidth changes, the session is permitted to continue over the fax codec (G.711). If the gatekeeper rejects the bandwidth increase, the fax codec is terminated and the gateway uses the configured fax protocol fallback or the original voice codec, in which case the fax transfer fails.

Configuring H.323 Fax Pass-Through

Cisco.com

To configure fax pass-through locally or globally, the following are required:

- **One or more individual VoIP dial peers**
- **VoIP dial peers globally configured**

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0—1-15

VoIP dial peers for fax or modem pass-through can be configured, one at a time or globally. If both methods are used, an individual dial-peer configuration takes precedence over the global configuration, which means that a call matching a particular dial peer tries first to apply the fax method that was configured individually on that dial peer. If no individual dial peer configuration was made, the router uses the global configuration.

When configuring dial peers, you have the choice of specifying fax pass-through or modem pass-through for the pass-through method. If you use the **fax protocol pass-through** command to specify fax pass-through as the method, the gateway uses the H.323 or SIP protocol stack to signal the changeover to fax mode. If you use the **modem passthrough** command to specify modem pass-through as the method, the gateway uses NSEs for fax changeover signaling.

Configuring One or More Individual VoIP Dial Peers

During this task, you enable fax pass-through on individual dial peers. Use the **fax protocol pass-through** command or the **modem passthrough** command, but not both.

Configuring VoIP Dial Peers Globally

If you are adding fax pass-through capability to a number of previously defined VoIP dial peers, you can configure all of them at one time in voice-service configuration mode.

Alternatively, you can add fax pass-through capability to VoIP dial peers one at a time by following the instructions in the “Configuring One or More Individual VoIP Dial Peers” available at

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/pt.htm#wp1125493>.

Note When fax pass-through or modem pass-through is configured under the dial-peer voice configuration, the configuration for an individual dial peer takes precedence over the global configuration under the **voice service voip** command.

When you are using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem pass-through with NSEs, you must also ensure that each incoming call is associated with a VoIP dial peer to retrieve the global fax or modem configuration. Associate calls with dial peers using the **incoming called-number** command to specify a sequence of digits that match incoming calls. Ensure that all calls match at least one dial peer by using the following commands:

- Router(config)# **dial-peer voice tag voip**
- Router(config-dial-peer)# **incoming called-number**

Configuring Fax Pass-Through on One or More Individual VoIP Dial Peers

Cisco.com

	Command or Action
Step 1	dial-peer voice tag voip Example: Router(config)# dial-peer voice 25 voip
Step 2	fax protocol pass-through {g711ulaw g711alaw} system or modem passthrough {system nse [payload-type number] codec {g711alaw g711ulaw} [redundancy]} Example: Router(config-dial-peer)# fax protocol pass-through g711ulaw or Router(config-dial-peer)# modem passthrough nse codec g711alaw redundancy
Step 3	fax-rate disable Example: Router(config-dial-peer)# fax-rate disable

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—1-16

The steps to configure fax pass-through on more than one dial peer are shown in the figure. Descriptions of the commands are in the “Configure Fax Pass-Through on One or More Individual VoIP Dial Peers” table.

Configure Fax Pass-Through on One or More Individual VoIP Dial Peers

Step	Command	Description
1.	<pre>dial-peer voice tag voip</pre> <p>Example:</p> <pre>Router(config)# dial-peer voice 25 voip</pre>	<p>Enters dial-peer configuration mode and defines a dial peer that directs traffic to or from a packet network.</p> <p>tag: This is a dial-peer identifier that consists of one or more digits. Valid entries are from 1 to 2147483647.</p> <p>voip: Calls from this dial peer use voice encapsulation on the packet network.</p>
2.	<pre>fax protocol passthrough {g711ulaw g711alaw} system</pre> <p>or</p> <pre>modem passthrough {system nse [payload-type number] codec {g711alaw g711ulaw} [redundancy]}</pre> <p>Example:</p> <pre>Router(config-dial-peer)# fax protocol passthrough g711ulaw</pre> <p>or</p> <pre>Router(config-dial-peer)# modem passthrough nse codec g711alaw redundancy</pre>	<p>Specifies the type of fax protocol to use on this dial peer.</p> <p>passthrough: Uses the H.323 or SIP protocol stack and the G.711 u-law or G.711 a-law codec. Use the same codec type for the originating and terminating gateways.</p> <p>system: Uses the protocol set under the voice-service configuration mode.</p> <p>Or</p> <p>Enables faxes to use modem pass-through and NSEs for fax changeover signaling. Keywords are as follows:</p> <p>system: Uses the protocol set under the voice-service configuration mode+.</p> <p>nse: Named Signaling Event (NSE) signaling is used to communicate codec switchover.</p> <p>payload-type number: (Optional) This is the value for the NSE payload type. Range varies by platform, but is from 96 to 119 on most platforms. Default is 100.</p> <p>codec: This is the codec selection for upspeeding. The default is g711ulaw. Use the same codec type for the originating and terminating gateways.</p> <p>g711alaw: G.711 a-law codec type for E1</p> <p>g711ulaw: G.711 u-law codec type for T1</p> <p>redundancy: (Optional) Enables a single repetition of packets (using RFC 2198) to protect against packet loss</p>
3.	<pre>fax-rate disable</pre> <p>Example:</p> <pre>Router(config-dial-peer)# fax-rate disable</pre>	<p>(Optional) This command disables fax protocol capability on this dial peer. Use this command only when you want to force faxes to use modem pass-through. Do not use this command when you want faxes to use fax pass-through or fax relay on this dial peer.</p>

Example: H.323 Fax Pass-Through

Cisco.com

```
Router# show running-config
Building configuration...
Current configuration:
. . . . .
!
voice service voip
h323
modem passthrough nse codec g711alaw redundancy sample-duration 20
!
. . . . .
dial-peer voice 500 voip
incoming called-number 800
destination-pattern 550
session target ipv4:10.100.00.00
fax rate disable
codec g726r32
!
gateway
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-17

The sample output in the figure displays a running configuration for fax pass-through with H.323 support.

Configuring MGCP Fax Pass-Through

Cisco.com

	Command or Action
Step 1	<code>no ccm-manager fax protocol cisco</code> Example: Router(config)# no ccm-manager fax protocol cisco
Step 2	<code>mgcp package-capability rtp-package</code> Example: Router(config)# mgcp package-capability rtp-package
Step 3	<code>mgcp modem passthrough voip mode nse</code> Example: Router(config)# mgcp modem passthrough voip mode nse
Step 4	<code>mgcp modem passthrough voip codec {g711ulaw g711alaw}</code> Example: Router(config)# mgcp modem passthrough voip codec g711alaw
Step 5	<code>mgcp modem passthrough voip redundancy [sample-duration [10 20]] [maximum-sessions sessions]</code> Example: Router(config)# mgcp modem passthrough voip redundancy sample-duration 20
Step 6	<code>mgcp timer nse-response t38 time</code> Example: Router(config)# mgcp timer nse-response t38 250
Step 7	<code>mgcp fax t38 inhibit</code> Example: Router(config)# mgcp fax t38 inhibit

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-1-18

Configuration of MGCP fax pass-through on Cisco voice gateways is similar to configuration of MGCP VoIP calls. Configuration is done by means of several commands in addition to a standard VoIP configuration. The same configuration must be present on the originating and terminating gateways. The “Configure MGCP Fax Pass-Through” table provides the required commands.

Configure MGCP Fax Pass-Through

Step	Action	Notes
1.	<pre>no ccm-manager fax protocol cisco</pre> <p>Example:</p> <pre>Router(config)# no ccm-manager fax protocol cisco</pre>	Turns off cisco fax relay, which is the default.
2.	<pre>mgcp package-capability rtp- package</pre> <p>Example:</p> <pre>Router(config)# mgcp package- capability rtp-package</pre>	Enables availability of the MGCP package for the RTP on the gateway.
3.	<pre>mgcp modem passthrough voip mode nse</pre> <p>Example:</p> <pre>Router(config)# mgcp modem passthrough voip mode nse</pre>	<p>Enables peer-to-peer RTP NSE signaling to coordinate the following between the originating and the terminating gateways:</p> <ul style="list-style-type: none"> ■ codec switchover ■ the disabling of the echo canceller and VAD.
4.	<pre>mgcp modem passthrough voip codec {g711ulaw g711alaw}</pre> <p>Example:</p> <pre>Router(config)# mgcp modem passthrough voip codec g711alaw</pre>	<p>(Optional) Specifies codec</p> <p>Keywords are as follows:</p> <p>g711ulaw: G.711 u-law codec type for T1</p> <p>g711alaw: G.711 a-law codec type for E1</p> <p>The default is g711ulaw.</p> <p>Note: Use the same codec type for both the originating and the terminating gateway.</p>
5.	<pre>mgcp modem passthrough voip redundancy [sample-duration [10 20]] [maximum-sessions sessions]</pre> <p>Example:</p> <pre>Router(config)# mgcp modem passthrough voip redundancy sample-duration 20</pre>	<p>(Optional) This command enables a single repetition of packets (using RFC 2198) to improve reliability by protecting against packet loss. When redundancy is on, all calls on the gateway are affected. Keywords are as follows:</p> <p>sample-duration: (Optional) This is the time length of the largest RTP packet when packet redundancy is active, in ms. Valid keywords are 10 and 20. Default: 10.</p> <p>maximum sessions sessions: (Optional) This is the maximum number of redundant sessions that can run simultaneously on each subsystem. The range varies by platform. For further information refer to the command line interface (CLI) help feature.</p>
6.	<pre>mgcp timer nse-response t38 time</pre> <p>Example:</p> <pre>Router(config)# mgcp timer nse-response t38 250</pre>	<p>(Optional) This configures a timeout period to wait for NSE responses from a peer gateway. The peer gateway either acknowledges the switchover and its readiness to accept packets or indicates that it cannot accept packets. The argument is as follows:</p> <p>time: Timeout period for awaiting NSE responses from a peer gateway, in ms. The range is 100 to 3000. The default is 200.</p>

Step	Action	Notes
7.	<code>mgcp fax t38 inhibit</code> Example: Router(config)# <code>mgcp fax t38 inhibit</code>	(Optional) This disables use of T.38 on the gateway. By default, T.38 is enabled.

Example: MGCP Fax Pass-Through

Cisco.com

```
Router# show running-config
!
voice call carrier capacity active
!
mta receive maximum-recipients 0
!
ccm-manager mgcp
no ccm-manager fax protocol cisco
!
controller T1 1/1
framing esf
linecode b8zs
ds0-group 0 timeslots 1 type e&m-
wink-start
. . . . .
```

```
mgcp mgcp call-agent 10.3.222.1 service-
type mgcp version 0.1
mgcp modem passthrough voip mode nse
mgcp package-capability rtp-package
mgcp fax t38 inhibit
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 3641 pots
application mgcpapp
port 3/0/0
!
dial-peer voice 3643 pots
application mgcpapp
port 1/1:0
!
gateway
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-19

The sample output in the figure displays a running configuration for fax pass-through with MGCP support.

Example: SIP Fax Pass-Through

Cisco.com

```
Router# show running-config
Building configuration...
Current configuration:
. . . . .
resource-pool disable
dial-tdm-clock priority 1 trunk-slot
1 port 0
spe link-info poll voice 5
spe default-firmware
spe-firmware-1
. . . . .
voice service voip
h323
modem passthrough nse codec g711alaw
redundancy sample-duration 20
!
no voice hpi capture buffer
no voice hpi capture destination
!
mrsp client session history duration
0
mrsp client session history records 0
memory check-interval 3600
memory validate-checksum 7200
```

```
redundancy
no keepalive-enable
mode classic-split
!
controller E1 0/0
pri-group timeslots 1-31
!
dial-peer voice 5001 pots
incoming called-number 550
destination-pattern 800
direct-inward-dial
port 0/0:D
prefix 800
!
dial-peer voice 500 voip
incoming called-number 800
destination-pattern 550
session target ipv4:10.100.00.00
session protocol sipv2
fax rate disable codec g726r32
!
gateway
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-20

The sample output in the figure displays a running configuration for fax pass-through with SIP support.

Fax Configuration Best Practices

This topic describes the best practices for configuring fax as voice in a VoIP environment.

Fax Considerations and Best Practices	
Cisco.com	
Cisco Fax Relay	<ul style="list-style-type: none">• Default, supported by H.323, sometimes SIP, not MGCP• Bandwidth and performance efficient• Requires Cisco platforms
T.38 Fax Relay	<ul style="list-style-type: none">• Bandwidth and performance efficient• Supported by H.323, sometimes SIP or MGCP• Standard supported in multi-vendor environment• Check platform support
Fax Pass-Through	<ul style="list-style-type: none">• Requires more bandwidth, size network accordingly• Supported by H.323, SIP, and MGCP• Very sensitive to packet loss, delay, and jitter• Supports any vendor fax

Best Practice: Cisco Fax Relay

- Use QoS to minimize packet loss, delay, and jitter.
- Use CAC.
- Disable call waiting on all dedicated modem and fax ports.
- Configure Cisco fax relay on originating and terminating gateways.

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-1-21

The following recommendations and guidelines can assist you in best implementing fax support on Cisco voice gateways:

- **Quality of service (QoS):** Use QoS to minimize the following:
 - **Packet loss:** Most fax machines appear to accept packet drop in the range of 0.4 percent to 0.6 percent without slowing down to the next speed. However, in a network with packet drop in the range of 0.8 percent to 1 percent, you should disable ECM. To improve performance in networks with a high frequency of out-of-order packet arrival, disable ECM on the fax machines. You can disable ECM on the gateway itself rather than disabling it on multiple fax machines. However, if packet drops occur, the fax image quality might deteriorate. Therefore, you should disable ECM only after considering whether you want to risk compromising image quality rather than experience longer call durations or dropped calls. You should also monitor and evaluate the network to identify and resolve the cause of the dropped packets.
 - **Delay:** Ensure that constant packet delay on the network does not exceed 1 second.
 - **Delay variation (jitter):** Ensure that delay variation (jitter) does not exceed 240 milliseconds.
- **CAC:** Use CAC to ensure that calls are not admitted if they exceed the specified total bandwidth limit.
- **Call waiting:** Disable call waiting on all dedicated modem and fax ports.
- **Cisco Fax Relay:** For best performance, verify that you have Cisco fax relay on both the originating and terminating gateways. If two Cisco IOS gateways have differing transports, they negotiate to use Cisco fax relay.

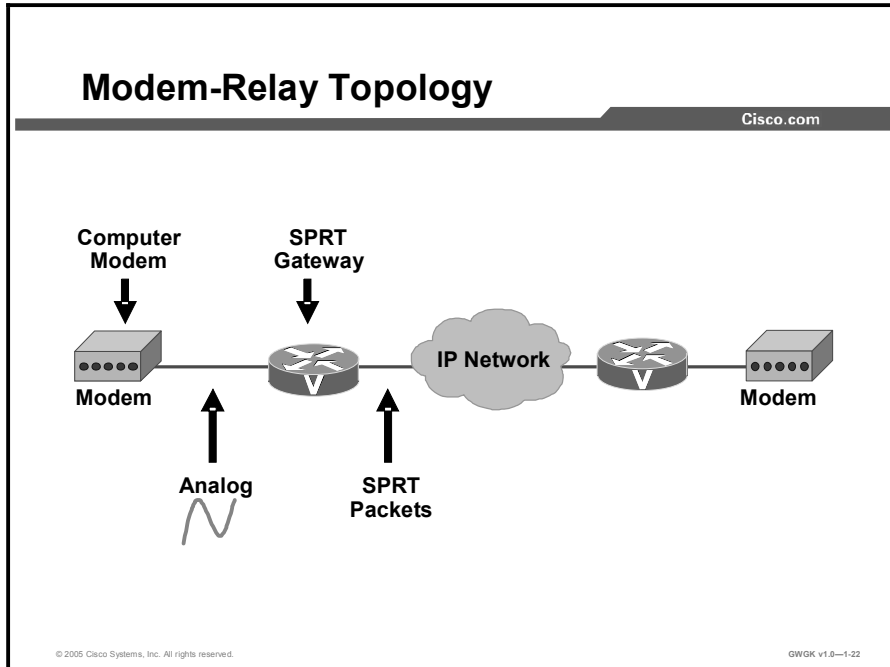
Note The only other gateway that does not support Cisco fax relay is the Cisco Digital Access DT-24/DE-30+. If you connect this gateway to a Cisco IOS gateway, you should configure both gateways to use fax pass-through mode.

For detailed information about implementing QoS in a Cisco IP telephony network, refer to *Cisco AVVID Network Infrastructure Enterprise Quality of Service Design* available at http://www.cisco.com/application/pdf/en/us/guest/netso/ns17/c649/cmigration_09186a00800d67ed.pdf.

Use the Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. You can access the Cisco Feature Navigator at <http://www.cisco.com/go/fn>.

Modem Relay

This topic explains the modem relay solution to the problem of modem as voice in a VoIP environment.



The modem-relay support on VoIP platforms provides support for modem connections across traditional time-division multiplexing (TDM) networks. When service providers implement VoIP, they sometimes cannot separate fax or data traffic from voice traffic. These carriers that aggregate voice traffic over VoIP infrastructures require service offerings to carry fax and data as easily as voice.

Starting on the left in the figure, modem relay demodulates a modem signal at one voice gateway and passes it as packet data to another voice gateway where the signal is remodulated and sent to a receiving modem. On detection of the modem answer tone, the gateways switch into modem pass-through mode and then, if the call menu signal is detected, the two gateways switch into modem-relay mode.

There are two ways to transport modem traffic over VoIP networks:

- With modem pass-through, the modem traffic is carried between the two gateways in RTP packets, using an uncompressed voice codec (G.711u-law or G.711a-law). Although modem pass-through remains susceptible to packet loss, jitter, and latency in the IP network, packet redundancy may be used to mitigate the effects of packet loss in the IP network.
- With modem relay, the modem signals are demodulated at one gateway, converted to digital form, and carried in Simple Packet Relay Transport (SPRT) protocol packets to the other gateway. At the destination gateway, the modem signal is re-created, remodulated, and passed to the receiving modem.

Note SPRT runs over UDP.

In this implementation, the call starts out as a voice call, switches into modem pass-through mode, and then switches into modem-relay mode. This feature significantly reduces the effects that dropped packets, latency, and jitter have on the modem session. Compared to modem pass-through, it also reduces the amount of bandwidth that is used.

A primary application of the modem-relay feature is the transport of modem dial-up traffic over IP networks.

Cisco Modem-Relay Features

Cisco.com

- **Modem tone detection and signaling**
- **Relay switchover**
- **Controlled redundancy**
- **Packet size**
- **Clock slip buffer management**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-23

Modem Tone Detection and Signaling

This implementation of modem relay supports V.34 modulation and the V.42 error correction and link-layer protocol with maximum transfer rates of up to 33.6 kbps. It also forces higher-rate modems to train down to the supported rates. Signaling support includes SIP, MGCP or SGCP, and H.323, and the gateways function as described here:

- For MGCP and SIP, during the call setup, the gateways negotiate the following:
 - To use or not use the modem-relay mode
 - To use or not use the gateway-xid
 - The value of the payload type for NSE packets
- For H.323, the gateways negotiate the following:
 - To use or not use the modem relay mode
 - To use or not use the gateway-xid

Relay Switchover

When the gateways detect a data modem, both the originating gateway and the terminating gateway switch to modem pass-through mode. This switch involves the following elements:

- Switching to the G.711 codec
- Disabling the high pass filter
- Disabling VAD
- Using special jitter buffer management algorithms
- Disabling the echo canceller on detection of modem phase reversal tone,

At the end of the modem call, the voice ports revert to the previous configuration, and the DSPs switch back to the state they were in before the switchover. You can configure the codec by selecting the **g711alaw** or **g711ulaw** option of the **codec** command.

Controlled Redundancy

You can enable payload redundancy so that the modem pass-through over VoIP switchover causes the gateway to send redundant packets. Redundancy can be enabled in one or both of the gateways. When only a single gateway is configured for redundancy, the other gateway receives the packets correctly but does not produce redundant packets.

Note By default, modem relay over VoIP capability and redundancy are disabled.

Packet Size

When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

Clock Slip Buffer Management

When the gateways detect a data modem, both the originating gateway and the terminating gateway switch from dynamic jitter buffers to static jitter buffers of 200-ms depth. The switch from dynamic to static is designed to compensate for PSTN clocking differences at the originating and terminating gateways. When the modem call is concluded, the voice ports revert to dynamic jitter buffers.

Modem-Relay Configuration Restrictions

Cisco.com

- **Confirm network suitability to relay modem traffic.**
- **Both gateways must have the following:**
 - **Modem relay enabled**
 - **At least Cisco IOS Software Release 12.2(11)T running on the gateways**
 - **High codec complexity configured for the originating and terminating gateways**
- **Both modems must have the following:**
 - **High-speed modems**
 - **V.42 error-correction protocol enabled**
 - **The error-correction layer enabled**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-24

Before you configure modem relay on the access server or gateway, make sure you have network suitability to relay modem traffic. The key attributes are packet loss, delay, and jitter. These characteristics of the network can be determined by using the Service Assurance Agent (SAA) feature in Cisco IOS software.

Modem relay works in the following situations:

- Modem relay is configured and enabled on both gateways.
- Cisco IOS Software Release 12.2(11)T must be running on the gateways.
- High codec complexity for the originating and terminating gateways is configured.
- Both modems are high-speed modems (such as V.34, V.90, or V.92) using V.42*bis* bidirectional compression. For low-speed modems, gateways carrying traffic use modem pass-through.
- Both modems use V.42 error correction protocol, and the error correction layer in both modems is enabled.

Note High-speed modems are modems that operate over normal dial-up telephone lines at speeds of 9600 bps and higher. They do not guarantee a specific throughput. Instead, they operate at a speed that depends on the quality of the line, the effectiveness of data compression algorithms on the data being transmitted, and other variables. These modems use hardware flow control to stop the data from reaching the host by toggling an EIA/TIA-232 signal when they cannot accept any more data.

Note MGCP, H.323, and SIP can be configured on the same gateway with some restrictions: All calls in a particular T1 or E1 must be handled by MGCP, H.323, or SIP. If your gateway has multiple T1 or E1 facilities then calls on some T1s or E1s can be managed by MGCP and others by H.323 or SIP.

Example: Modem-Relay Using an H.323 Configuration

Cisco.com

```
Router# show running-config
!
voice service voip
  modem relay nse codec g711ulaw
  redundancy maximum-session 5
!
resource-pool disable
!
!
mta receive maximum-recipients 0
!
controller T1 0
  framing esf
  clock source line primary
  linecode b8zs
  pri-group timeslots 1-24
```

```
!
voice-port 0:D
!
dial-peer voice 1 pots
  incoming called-number
  55511..
  destination-pattern 020..
  direct-inward-dial
  port 0:D
  prefix 020
!
dial-peer voice 2 voip
  incoming called-number 020
  destination-pattern 55511..
  modem relay nse codec g711ulaw
  redundancy
  session target ipv4:26.0.0.2
!
```

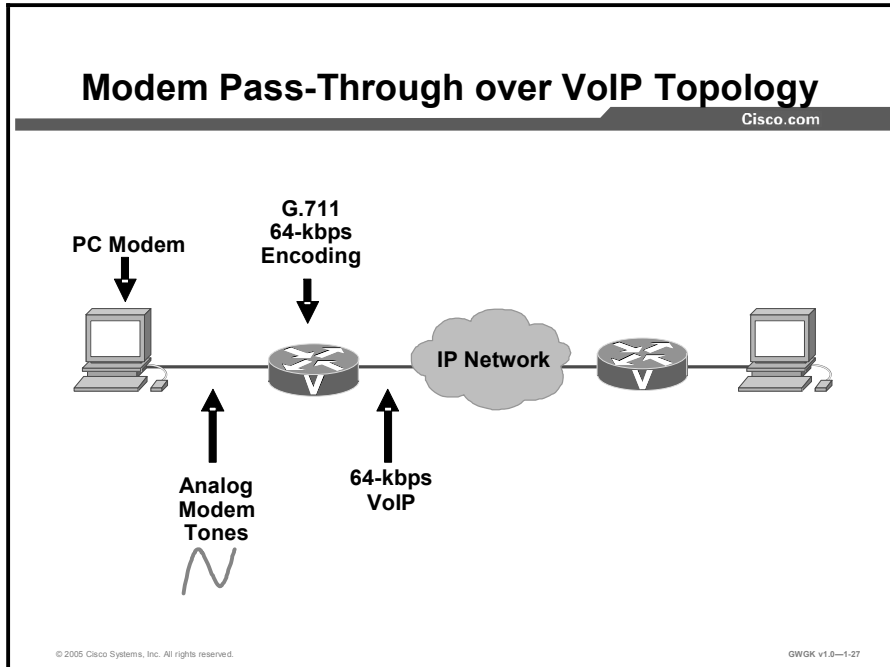
© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-1.28

The screen capture shows a sample configuration for H.323 modem relay over VoIP. The commands to enable modem fax relay features are highlighted in the screen capture.

Modem Pass-Through

This topic explains the modem pass-through solution to the problem of modem as voice in a VoIP environment.



The figure shows a typical modem pass-through network topology. The PC modem sends analog modem tones to the gateway. The gateway encodes the data stream using G.711 64-kbps encoding. In this way, the gateway allows the transport of a modem session across a VoIP network using G.711 frames, which turns off echo cancellation, voice activity detection, and comfort noise generation. The process is reversed when the modem data stream reaches the receiving side of the network.

Note The Internet Engineering Task Force (IETF) RFC 2198 on packet redundancy enhances modem pass-through reliability.

Gateway Support for Modem Pass-Through Features

Cisco.com

- **Repressing processing functions**
- **Issuing redundant packets**
- **Providing static jitter buffers**
- **Differentiating modem signals from voice and fax signals**
- **Maintaining a modem connection reliably across the packet network**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1.28

Modem pass-through performs the following functions:

- Represses processing functions like compression, echo cancellation, high-pass filter, and VAD.
- Issues redundant packets to protect against random packet drops.
- Provides static jitter buffers of 200 ms to protect against clock skew.
- Differentiates modem signals from voice and fax signals. This function indicates the detection of the modem signal across the connection, and places the connection in a state that transports the signal across the network with the least distortion.
- Maintains a modem connection reliably across the packet network for a long duration under normal network conditions.

Note In general, modem pass-through and modem relay are the mechanisms for supporting modem sessions over an IP network that uses voice gateways.

Modem Pass-Through Configuration

Cisco.com

```
Router# show running-config
Building configuration...
Current configuration:
.
.
.
!
voice service voip
modem passthrough nse codec g711ulaw redundancy maximum-session 5
!
resource-pool disable
!
.
.
.
dial-peer voice 2 voip
incoming called-number 020..
destination-pattern 55511..
modem passthrough nse codec g711ulaw redundancy
session target ipv4:26.0.0.2
!
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-29

The example in the figure shows a sample configuration for modem pass-through:

For information on a simple modem pass-through configuration in “Cisco IP Telephony Solution Reference Network Design (SRND) Cisco CallManager Release 4.0”, go to http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a00802c370c.html.

Modem Relay and Modem Pass-Through

Cisco.com

Modem Relay	<ul style="list-style-type: none">• Default, supported by H.323, sometimes SIP, not MGCP• Bandwidth and performance efficient• Requires Cisco platforms
Modem Passthrough	<ul style="list-style-type: none">• Requires more bandwidth; size network accordingly• Supported by H.323, SIP, MGCP• Very sensitive to packet loss, delay, jitter

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-30

The table in the figure compares the feature of modem relay to the features of modem pass-through.

Modem Configuration Best Practices

This topic describes the best practices for configuring a modem as voice in a VoIP environment.

Modem Configuration Best Practices

Cisco.com

- **Use QoS to minimize packet loss, delay, and jitter**
- **Use CAC**
- **Disable call waiting on all dedicated modem and fax ports**
- **Configure modem relay on both gateways**
- **Use a single signaling protocol and gateway family**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0—1-31

Observe the following recommended best practices to ensure optimum performance of modem traffic transported over an IP infrastructure:

- Ensure that the IP network is enabled for QoS and that you adhere to all of the recommendations for providing QoS in the LAN, metropolitan-area network (MAN), and WAN environments. Every effort should be made to minimize the following parameters:
 - **Packet loss:** Fax and modem traffic requires an essentially loss-free transport. A single lost packet results in retransmissions.
 - **Delay**
 - **Delay variation (jitter)**
- Disable call waiting on all dedicated modem and fax ports.
- Use CAC to ensure that calls are not admitted if they exceed the specified total bandwidth limit.
- Use G.711 for all calls involving a modem. If one of the gateways does not support modem relay, modem pass-through is negotiated (G.711 only). If modems are used, the best-practice recommendation is to use G.711 for all calls.
- Where possible, use a single signaling protocol and gateway family to minimize interoperability issues.
- Disable call waiting on all dedicated modem and fax ports.

Caution Do not use the IP network to connect modems that will be used to troubleshoot or diagnose problems with the IP network. In this case, the modems that are used to troubleshoot the devices that compose the IP infrastructure should be connected to a POTS.

Note For more information, refer to the *Cisco AVVID Network Infrastructure Enterprise Quality of Service Design* available at http://www.cisco.com/application/pdf/en/us/guest/netsol/ns17/c649/ccmigration_09186a00800d67ed.pdf.

Modem Pass-Through Best Practices

Cisco.com

- Follow modem relay QoS best practices
- Use CAC
- Disable call waiting on all dedicated modem and fax ports
- Use G.711 for all calls involving a modem
- Use a single signaling protocol and gateway family

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-32

Observe the following recommended best practices to ensure optimum performance of modem traffic transported over an IP infrastructure:

- Ensure that the IP network is enabled for QoS following the same QoS best practices for modem relay.
- Use CAC to ensure that calls are not admitted if they exceed the specified total bandwidth limit.
- Use G.711 for all calls involving a modem. If one of the gateways does not support modem relay, modem pass-through is negotiated (G.711 only). If modems are used, the best-practice recommendation is to use G.711 for all calls.
- Where possible, use a single signaling protocol and gateway family to minimize interoperability issues.
- Disable call waiting on all dedicated modem and fax ports.

Caution Do not use the IP network to connect modems that will be used to troubleshoot or diagnose problems with the IP network. In this case, the modems used to troubleshoot the devices that compose the IP infrastructure should be connected to a POTS.

Note Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Cisco fax relay and T.38 fax relay protocols terminate modulated fax signals, extract digital information, and relay digital information through a data network using data packets. At the terminating side, digital information is extracted from the packet, modulated, and played out.**
- **Faxes can be transmitted successfully when codecs such as G.726 and G.711, with no echo cancellation or VAD, are used. This method of sending faxes through the voice codec is usually referred to as in-band faxing or fax pass-through.**
- **Fax pass-through occurs when incoming fax data is not demodulated or compressed for its transit through the packet network. Using fax pass-through, two fax machines communicate directly with each other over a transparent IP connection.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-33

Summary (Cont.)

Cisco.com

- **Modem relay occurs when modem signals are demodulated at one gateway, converted to digital form, and carried in SPRT packets to another gateway where the modem signal is recreated, remodulated, and passed to the receiving modem.**
- **With modem passthrough, the modem traffic is carried between the two gateways in RTP packets using an uncompressed voice codec**
- **Fax and modem relay and passthrough are all configured at the dial-peer prompt.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—1-34

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) Describe the similarities between Cisco fax relay and T.38 fax relay. (Source: Fax Relay)

- Q2) When is fax pass-through used? (Source: Fax Pass-Through)
- A) Fax pass-through is used when incoming fax data is not demodulated or compressed for its transit through the packet network.
 - B) Fax pass-through is always used; it is the default mode for passing faxes through a VoIP network, and Cisco fax pass-through is the default fax pass-through type.
 - C) Fax pass-through is used when incoming fax data needs to be “hairpinned” back out to the PSTN without passing through the network.
 - D) Fax pass-through is used when the gateway needs to break down T.30 fax tones into their specific HDLC frames for transmission across the VoIP network.
- Q3) What type of connection is needed for two fax machines using fax pass-through to communicate? (Source: Fax Pass-Through)
- A) an IPSec-based connection
 - B) a VoIP connection
 - C) a transparent IP connection
- Q4) What two things must be in place for gateway support of modem relay? (Choose two.) (Source: Modem Relay)
- A) Both modems must be high-speed modems using at least V.42*bis* bidirectional compression.
 - B) Cisco IOS Software Release 12.2(11)T must be running on the gateways.
 - C) The gateway must support channel-associated signaling to allow the fax tones to be encoded on the link.
 - D) Modem relay must be enabled on both gateways. However, the default configuration is sufficient.
 - E) The gateway must have sufficient DSP resources on the multiflex trunk card to encode the modem-relay tones into the appropriate codec.
 - F) Both modems must be high-speed modems capable of encoding and decoding V.32*bis* symbols.
 - G) Modem relay must be configured and enabled on both gateways.

- Q5) The debugs from a gateway reveal that T.38 negotiation fails and the call reverts to an audio codec. What is the reason? (Source: Fax Relay)
- A) SIP T.38 fax relay is not supported by both gateways.
 - B) SIP T.38 has been configured at each end with conflicting parameters.
 - C) T.38 is not a supported fax protocol.
 - D) One gateway is running T.38v3, so the other must be upgraded to Cisco IOS Software Release 12.2(11)T or later.
- Q6) How much bandwidth does T.38 fax relay require? (Source: Fax Relay)
- A) 56-kbps transmission rate
 - B) 32-kbps transmission rate
 - C) 128-kbps transmission rate
 - D) 64-kbps transmission rate

Lesson Self-Check Answer Key

- Q1) Cisco fax relay and T.38 fax relay terminate the modulated fax signal, extract the digital information, and then relay the digital information through the data network using data packets. At the terminating side, the digital information is extracted from the packet, modulated, and played out.
- Q2) A
- Q3) C
- Q4) A, G
- Q5) A
- Q6) D

Module Summary

This topic summarizes the key points discussed in this module.

Module Summary

Cisco.com

- Gateways connect two different types of networks.
- The differences in the voice gateway protocols provide a basis for selection.
- H.323 is a robust, peer-to-peer gateway protocol that serves the needs of TDM interworking very well.
- MGCP is suited to scalability and survivability.
- SIP perform many of the functions of H.323 with the added benefit of high extensibility because of the ease of development of SIP-related applications.
- MGCP-controlled backhaul of BRI signaling provides service to remote office gateways that connect via ISDN BRI trunks to a centralized Cisco CallManager.
- Support for fax and modem remains a challenge for system administrators. The relay and pass-through systems are activated through dial-peer configuration commands.

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-1.1

The implementation of gateways is critical to the success of VoIP or an IP telephony solution. The module covered the concepts involved with gateway deployment, including the selection of the protocol that you will deploy, the routes that you set up on the dial peers or in CallManager, and how you handle issues such as a lack of DTMF tones or problems sending or receiving faxes.

References

For additional information, refer to these resources:

Cisco CallManager

- *A Typical U.S. Dial Plan for Cisco CallManager 3.x and 4.x.*
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a0080094b2a.shtml.
- *Cisco CallManager Administration Guide Release 4.1(1).*
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_administration_guide_book09186a00802d8eaf.html.
- *Cisco CallManager and Cisco IOS Interoperability Configuration Guide.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/ccm_c/index.htm.
- *Cisco CallManager Express (CME) 3.0 Design Guide.*
http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/its30/cme30dg.htm

- *Cisco CallManager Express 3.0 System Administrator Guide.*
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5012/products_feature_guide_book09186a00801812e4.html.
- *Cisco CallManager Security Guide Release 4.1(2).*
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/ae/sec412/index.htm.
- *Cisco CallManager System Guide Release 4.1(2).*
http://www.cisco.com/en/US/products/sw/voicew/ps556/products_administration_guide_book09186a00802d8ff6.html.
- *Cisco IP Telephony Solution Reference Network Design (SRND) Cisco CallManager Release 4.0.*
http://www.cisco.com/en/US/products/sw/voicew/ps556/products_implementation_design_guide_book09186a00802c370c.html.
- *Configuring MGCP PRI Backhaul and T1 CAS Support for Cisco CallManager.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/ccm_c/intcnf3.htm.
- *Overview of Cisco CallManager and Cisco IOS Interoperability.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/ccm_c/interovr.htm.

Fax and Modems

- *Cisco Fax Services over IP Application Guide.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide_book09186a008017cf32.html.
- *Modem Support for VoIP.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/vclmodem.htm.

H.323

- *Cisco H.235 Accounting and Security Enhancements for Cisco Gateways.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800b5d51.html.
- *Cisco IOS H.323 Gateway Configuration for Use with Cisco CallManager.*
http://www.cisco.com/en/US/products/sw/voicew/ps556/products_tech_note09186a0080094636.shtml.
- *Configuring H.323 Gateways.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_chapter09186a00802b45e0.html.
- *H.323 and SIP Integration.*
http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a0080092947.shtml.
- *H.323 Gateway Dial-Peer Configuration for Cisco CallManager Server Redundancy.*
http://www.cisco.com/en/US/products/sw/voicew/ps556/products_configuration_example09186a0080094852.shtml.
- *H.323 Version 2 Support.*
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xh/h323v2xh.htm>.

- *Understanding H.323 Gatekeepers.*
http://www.cisco.com/en/US/tech/tk652/tk701/technologies_tech_note09186a00800c5e0d.shtml.

IOS Command References

- *Cisco IOS Debug Command Reference, Release 12.3.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a008017cf4d.html.
- *Cisco IOS Dial Technologies Configuration Guide, Release 12.2.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080393bf3.html.
- *Cisco IOS Security Configuration Guide, Release 12.3*
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d583.html.
- Cisco IOS Software. <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml>.
- *Important Information on Debug Commands.*
http://www.cisco.com/en/US/tech/tk801/tk379/technologies_tech_note09186a008017874c.shtml.

IOS Voice

- *Cisco IOS Voice Command Reference, Release 12.3.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a00801e8a79.html.
- *Cisco IOS Voice Configuration Library.*
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vcl.htm>.
- *Cisco IOS Voice Troubleshooting and Monitoring Guide.*
http://cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/voipt_c/index.htm.
- *Cisco IOS Voice, Video, and Fax Configuration Guide Release 12.2.*
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ada.html.
- *Understanding Cisco IOS Gatekeeper Call Routing.*
http://www.cisco.com/en/US/tech/tk652/tk701/technologies_tech_note09186a00800a8928.shtml.

MGCP

- *Cisco IOS MGCP and Related Protocols Configuration Guide.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a008020bd29.html.
- *Configuring Cisco CallManager with IOS MGCP Gateways (Analog FXO, FXS Ports).*
http://www.cisco.com/en/US/products/sw/voicew/ps556/products_tech_note09186a008009428e.shtml.
- *Configuring MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco CallManager.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_c/ccm_c/int_bri.htm.

- *How to Configure MGCP with Digital PRI and Cisco CallManager.*
http://www.cisco.com/en/US/tech/tk652/tk701/technologies_configuration_example09186a00801ad22f.shtml.
- *Interworking of Cisco MGCP Voice Gateways and Cisco CallManager Version 3.2.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800b65dd.html.
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gtsecure.htm.
- IETF.org. *Media Gateway Control Protocol (MGCP) Version 1.0.*
<http://www.ietf.org/rfc/rfc3435.txt>.
- *Understanding MGCP Interactions with Cisco CallManager.*
http://www.cisco.com/warp/public/788/AVVID/understanding_mgcp.html.

SIP

- *Cisco IOS SIP Configuration Guide.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_c/sip_c/sipc1_c/index.htm.
- *Configuring SIP ISDN Support Features.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_c/sip_c/sipc1_c/chapter8.htm.
- *Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms.*
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftsipgv1.htm>.
- *Guide to Cisco Systems' VoIP Infrastructure Solution for SIP Version 1.0.*
<http://www.cisco.com/univercd/cc/td/doc/product/voice/sipsols/biggulp/>.
- *Preparing Cisco SRST Support for SIP.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/srst32ad/srs_sip.htm.
- IETF.org. *SIP: Session Initiation Protocol.* <http://www.ietf.org/rfc/rfc2543.txt>.

VoIP

- *Cisco - VoIP Toll Bypass Application for International Bank.*
http://www.cisco.com/en/US/tech/tk652/tk701/technologies_configuration_example09186a0080094b97.shtml.
- *Configuring Voice over IP.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca6a2.html.
- *Service Provider Features for Voice over IP.*
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/voip1203.htm>.
- *Voice Design and Implementation Guide.* <http://www.cisco.com/warp/public/788/pkt-voice-general/7.html>.

- *Voice Network Signaling and Control.*
http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800a6210.shtml#Topic4.
- *Voice Over IP - Per Call Bandwidth Consumption.*
http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml.

Module 2

Integrating a VoIP Network to the PSTN and PBXs

Overview

This module is about the circuits that connect the Cisco gateway either to the public switched telephone network (PSTN) or to PBXs. Because analog fax machines are still in operation, the module describes analog circuits, channel associated signaling (CAS), and PRI T1 circuits. This module also describes what happens when you introduce Q Signaling (QSIG), the language of the PBX, to the telephony network.

Module Objectives

Upon completing this module, you will be able to identify the requirements for integrating a VoIP network with the PSTN and PBXs using voice gateways. This ability includes being able to meet these objectives:

- Describe the activities that are required to integrate gateways into PSTN and PBX circuits
- Integrate a voice gateway into the PSTN or a PBX using analog circuits
- Integrate a voice gateway into the PSTN or a PBX using CAS circuits
- Integrate a voice gateway into the PSTN or a PBX using PRI circuits
- Integrate a voice gateway into the PSTN or a PBX using QSIG

Lesson 1

Connecting to the PSTN and PBXs

Overview

This lesson provides an overview of how to connect voice gateways to an existing telephony system. The purpose of the lesson is to introduce the analog and digital trunking options that will be presented later in the module.

Objectives

Upon completing this lesson, you will be able to describe the activities that are required to integrate gateways into PSTN and PBX circuits. This ability includes being able to meet these objectives:

- Describe the common PSTN and PBX circuit options that are available for deployment on a voice gateway
- Describe PSTN and PBX telephony circuit options for integration with voice gateways
- Describe PSTN and PBX integration requirements for deploying analog and digital circuits on a voice gateway
- Describe common analog circuit characteristics
- Describe common digital circuit characteristics
- Describe additional considerations required for a PBX integration on a voice gateway

Overview of PSTN and PBX Circuit Options

This topic describes the common public switched telephone network (PSTN) and PBX circuit options that are available for deployment on a gateway.

Overview of PSTN and PBX Circuit Options			
Type	Circuit Option	Comments	
Analog	Subscriber loop	• Low cost	
	E&M	• Potentially low cost	
Digital	T1 CAS E1 R2	• Reasonably priced • Can provide ANI	
	ISDN	T1 PRI	• More services than CAS
		E1 PRI	• Common on modern PBXs
	BRI	• Mostly for EMEA	
QSIG	• Created for interoperation of PBXs from different vendors • Rich in supplementary services		

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-2.3

The two circuit options that are available are analog and digital. The advantages and shortcomings of individual analog and digital circuit options that can be deployed in Cisco voice gateways are summarized in the following list:

- **Subscriber loop:** Subscriber loop is usually a low-cost solution and is used when traditional phones connect directly to a voice gateway with a Foreign Exchange Station (FXS) interface. The two types of interfaces that make up subscriber loop trunks are the following:
 - **Foreign Exchange Office (FXO):** Use FXO ports to connect to a central office (CO), PBX, or key telephone system. You can configure loop-start or ground-start signaling interfaces, depending on the model of voice interface card or network module selected.

Note Cisco CallManager assumes all loop-start trunks lack positive disconnect supervision. Cisco recommends that you configure trunks with positive disconnect supervision such as ground start.

- **FXS:** Use FXS ports to connect to any plain old telephone service (POTS) device such as analog phones, fax machines, and legacy voice-mail systems.
- **RecEive and transMit (E&M) interfaces:** E&M signaling is commonly referred to as “ear and mouth” or “recEive and transMit”, but its origin comes from the term earth and magneto. “Earth” represents electrical ground and “magneto” represents the electromagnet used to generate tone. E&M allows extension dialing before the conversation begins. E&M is a low-cost trunking solution, but it requires a special interface card for the PBX. If the PBX is already equipped with this card, E&M can be an even lower-cost solution.

- **T1 or E1 channel associated signaling (CAS) trunk:** There are many CAS variants that operate over analog and digital interfaces. A common digital interface that is used is T1 or E1 (European version), where each channel includes a dedicated signaling element. The type of signaling most commonly used with T1 CAS is E&M signaling.
- **ISDN:** In addition to the calling party identification service provided by CAS trunks, supplementary services such as call waiting and do not disturb are available with ISDN. ISDN can be setup with a BRI, which is rarely offered by North American telephone companies. BRI allows up to two simultaneous calls. A second type of circuit option with ISDN is the PRI. PRI allows up to 24 simultaneous calls over T1 or 30 simultaneous calls over E1. An interface card supporting PRI is usually already in place on modern PBXs. The PRI interface is economically preferable to BRI when more than eight channels (4xBRI) are required. These are the two worldwide standards for PRI:
 - **T1-PRI:** Use this interface to designate North American ISDN PRI with 23 bearer channels and one common channel signaling (CCS) channel.
 - **E1-PRI:** Use this interface to designate European ISDN PRI with 30 bearer channels, one CCS channel, and one framing channel.
- **ISDN with Q Signaling (QSIG):** QSIG is an International Organization for Standardization (ISO) standard. QSIG enables supplementary features between PBXs from different manufacturers. QSIG is used to interconnect PBXs.

PSTN and PBX Circuit Options with Cisco Voice Gateways

Cisco.com

Circuit Type	Gateway type:		Connects to:		
	MGCP	H.323 or SIP	PBX	Key Telephone System	PSTN
Analog E&M		X	X	X	
Analog FXO	X	X	X	X	X
Analog DID		X			X
Analog CAMA		X			X
BRI Q.931 Network Side	X	X	X	X	
BRI Q.931 User Side		X			X
BRI QSIG		X	X	X	
T1 CAS E&M (wink-start and immediate start)	X	X	X	X	X
T1 CAS E&M (delay dial)		X	X	X	X
T1 CAS FGD		X	X		X
T1 CAS FXO (ground-start and loop-start)		X	X	X	X
T1 CAS FXS (ground-start and loop-start)		X	X	X	
E1 CAS, E1-Me1CAS, E1 R2		X	X		X
T1 or E1 ISDN PRI Q.931	X	X	X	X	X
T1 or E1 QSIG basic	X	X	X		

© 2005 Cisco Systems, Inc. All rights reserved.

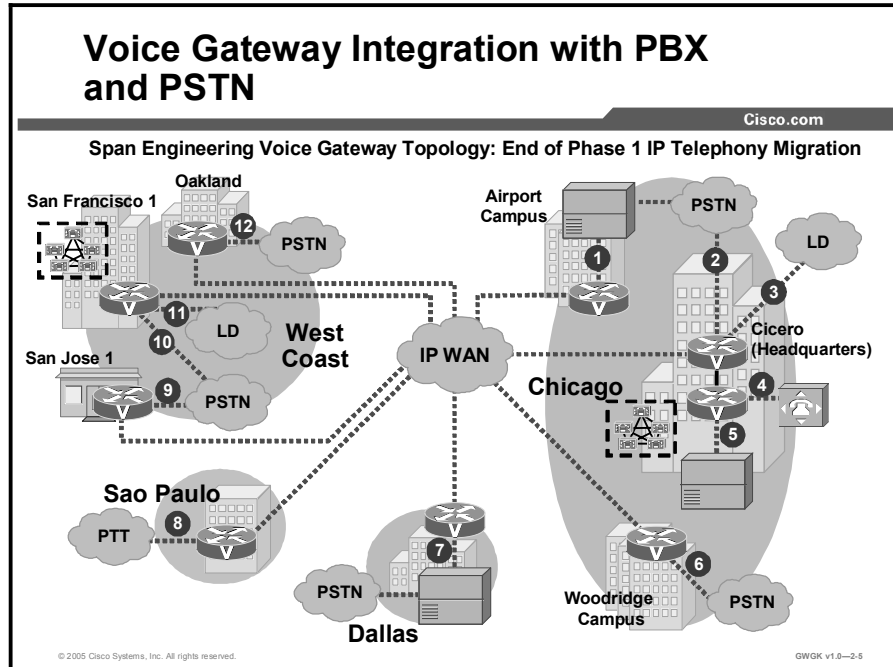
GWGK v1.0-2.4

Cisco voice gateway routers support the circuit types described in this figure. Both Centralized Automatic Message Accounting (CAMA) and Feature Group-D (FGD) are further described in the lesson “Analog Circuits.”

Note The Media Gateway Control Protocol (MGCP) limits that are listed in the figure are for Cisco CallManager and not for the MGCP gateways.

PSTN and PBX Integration Overview

This topic describes PSTN and PBX telephony circuit options that are available for integration with voice gateways.



This figure shows how one organization, Span Engineering, has deployed voice gateways to integrate with the PSTN and a PBX. The table "Span Engineering Configuration" describes the topology.

Span Engineering Configuration

Connection	Connects Gateway to	Description	Gateway Recommended by Designer
1	Nortel Meridian Opt 11c	4 x T1 CAS	2 x VWIC-2MFT-T1 in a 2811
2	PSTN	8 x T1 PRI	WS-6608-T1
3	Long distance	5 x T1 PRI	WS-SVC-CMM-6T1
4	Panasonic PBX	3 x T1 PRI	VVIC-1MFT-T1 in a 3825
5	Nortel Meridian 1 Release 25	4 x T1 PRI	2 x NM-HDV-2T1-48 in a 3825
6	PSTN	3x T1 PRI	2 x NM-HDV-2T1-48 in a 3845
7	Avaya Definity G3si	3 x T1 PRI	2 x NM-HDV-2T1-48 in a 3845
8	Post, Telephone, and Telegraph (PTT) and private integrated services network (PISN)	1 x E1 R2 and 1 x E1 PRI	NM-HDV-2E1-60in a 3845
9	PSTN	2 x BRI	VIC2-2BRI-NT/TE in a 2811

Connection	Connects Gateway to	Description	Gateway Recommended by Designer
10	PSTN	4 x T1 PRI	4 ports on WS-6608-T1
11	Long distance	4 x T1 PRI	4 ports on WS-6608-T1
12	PSTN	1 x T1 PRI	VVIC-1MFT-T1 in a 2821

The most difficult part of integrating a Cisco voice gateway with a PBX is finding a common ISDN protocol that supports all the required telephone features the PBX has been providing. With some combinations of gateways and PBXs, this can be even more complicated because the feature support may depend on whether you can configure either the gateway or the PBX for the network side or user side. For example, the only Nortel PBX that can currently support calling number identification (CNID) interoperability with Cisco routers is the DMS100. DMS100 cannot be configured as network side; therefore, integration requires that you configure the Nortel device for the SL1 network side and the Cisco router for the DMS100 user side.

Note SL1 is the Nortel CO variant of the DMS100 protocol.

PSTN and PBX Integration Requirements

This topic describes PSTN and PBX integration requirements for deploying analog and digital circuits on a gateway.

PSTN and PBX Integration Considerations

Cisco.com

Factors influencing interface configuration

- **Top-down or bottom-up integration**
- **Provisioning specifications**
 - **Clocking**
 - **Framing**
 - **Line coding**
 - **Line levels**
- **Support for proprietary signaling or connection types**
- **Match the PBX configuration**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.8--2.6

The following are key considerations for PSTN and PBX integration:

- **Top-down or bottom-up:** A top-down approach means working from the highest priority call to the lowest priority, and a bottom-up approach means working from the lowest priority to highest priority. For these approaches, you need to consider where the move toward integration originated. For example, an organization may want to pursue integration as a business strategy or as the result of a push from the information technology (IT) department. The integration team can use this information to build communication strategies to mitigate the issues associated with either integration approach.
- **Provisioning specifications:** Clocking issues are typical of the problems associated with integrating a PSTN and PBX. For example, when selecting the type of signaling interface, consider which ones run on internal clocking rather than service provider clocking. PSTN and PBX integration require network termination 1 (NT-1) terminations for BRI trunks and channel service units (CSUs) for digital T1 connections. If the service provider equipment does not provide either of these terminations, you must provide them. Finally, if integration with the PSTN or a PBX requires a signaling change, be aware of the effect that a change in signaling will have on the entire network.
- **Support of proprietary signaling or connection types:** Determine if the gateway needs to support any proprietary signaling or connection types to the PBX.
- **PBX configuration support:** The following presents the key information required to ensure that a Cisco voice gateway can be configured to support calls from a legacy PBX:
 - E&M signaling type (I, II, III, or V)
 - Audio implementation (2-wire or 4-wire)
 - Start dial supervision (wink-start, immediate, or delay-dial)
 - Dial method (dual tone multifrequency [DTMF] or pulse)
 - Call progress tones (standardized within geographic regions)
 - PBX port impedance

Analog Integration Characteristics

This topic describes common analog circuit characteristics.

Analog Signaling

Cisco.com

These are the characteristics of analog signaling:

- **One voice channel per circuit**
- **Analog signal is subject to attenuation**
- **A limited feature set**
- **Low cost**

Analog Signaling includes the following:

- **Subscriber Loop**
 - **Loop-start**
 - **Ground-start**
- **E&M**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-2.7

There is one voice channel per analog circuit; therefore, density of traffic on the physical plant is limited. Although analog signaling has evolved to include several features such as caller ID, call waiting, transfer, and conference, the feature set is limited when compared to CAS or ISDN. The limited set of features associated with analog signaling is inexpensive.

A subscriber loop is a two-wire interface used primarily when connecting a telephone set to a Subscriber Line Module-Analog (SLMA) interface channel in a PBX. The SLMA corresponds to a FXS module in a Cisco voice gateway. FXS and Subscriber Line Interface Circuit (SLIC) emulation modules can also be interconnected to a Trunk Module-Analog (TMA) interface channel in the PBX. This corresponds to an FXO module in a Cisco voice gateway. The following describes the operating modes for subscriber loops:

- **FXO or TMA telephone emulation:** In this mode, the terminal equipment, which could be either the PBX or the voice gateway, can only detect a ringing signal, provide digit dialing, and provide switching between off-hook and on-hook.
- **FXS or SLMA SLIC emulation:** In this mode, the SLMA or FXS module waits for a closed loop that generates a current flow and a signaling tone of 425 Hz. The SLIC provides battery, overvoltage, ringing, supervision, hybrid 2/4 wires, and testing functions.

The Cisco analog E&M interface functions as the signaling-unit side, and the other side is expected to be a trunk circuit. When using E&M interface models Type II and Type V, two signaling-unit sides can be connected back-to-back by crossing the signaling leads. When you are using E&M Type I and Type III interfaces, two signaling-unit sides cannot be connected back-to-back.

Many PBX brands have E&M analog trunk cards that can operate as either the trunk-circuit side or the signaling-unit side. Because the Cisco E&M interfaces are fixed as the signaling-unit side of the interface, it may be necessary to change the E&M trunk settings on the PBX to operate as the trunk-circuit side. The only way that the PBX works with the Cisco E&M interface is if you use Type I or III E&M settings.

If a PBX or a key system can operate only as the signaling-unit side of the E&M interface, it cannot interoperate with the Cisco E&M interface if Type I or Type III is chosen. PBX products fixed as the signaling-unit side can be used with the Cisco E&M interface if Type II or Type V E&M is used.

Digital Integration Characteristics

This topic describes common digital circuit characteristics.

Digital Integration Characteristics

Cisco.com

Digital Circuits have these characteristics:

- **More calls simultaneously**
- **Signal amplification**
- **Caller identification**
- **Network emulation**
- **Clocking**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-2.8

Digital circuits have the following characteristics:

- Digital circuits provide greater traffic density on the physical plant than with analog circuits do.
- Digital signals can be perfectly amplified so that signals can be restored. Therefore, distance from end-to-end becomes unimportant for successful completion of a call.
- The passage of caller identification in the digital network enables control features like billing for services used.
- Network-side ISDN PRI enables the access gateway to provide a standard ISDN PRI network-side interface to the PBXs and to mimic the behavior of legacy phone switches. The access server functions as a National ISDN PRI switch or a European Telecommunication Standards Institute (ETSI) PRI Net5 switch to a PBX.
- For voice data to travel over an IP network, it must be packaged, sent out over the physical layer of the network, unpackaged, and recreated as an analog signal to be heard. The packing and unpacking techniques use the frequency of a digital clock to coordinate this process. Consequently, care must be taken to ensure all equipment that participates in a VoIP call is synchronized to the same clock source; otherwise, voice transmissions become garbled. This timing problem does not exist with analog trunks.

PBX Integration Considerations

This topic describes the additional considerations required for PBX integration.

PBX Integration Requirements

Cisco.com

- **Legacy upgrades**
- **Dial plans**
- **Trunk reconfiguration**
- **Voice-mail integration**
 - **Traditional voice mail with IP phones**
 - **Cisco Unity with traditional phones**
 - **Cisco Unity and traditional voice mail both deployed**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0--2-9

The following describes the key considerations when implementing an IP telephony migration plan, or even simply integrating VoIP into a PBX, key system, voice-mail system, or a legacy messaging system:

- **Legacy upgrades:** Upgrading the legacy PBX or key system with such components as software and voice cards may be required so that the legacy system can be integrated with the new solution.
- **Dial plans:** Examine the existing dial plan, and identify and plan the modifications that may be required to the master dial plan and within the PBX programming.
- **Trunk reconfiguration:** An integrated system may require trunk or channel reconfiguration.
- **Voice-mail integration:** If legacy voice-mail integration is being considered, Audio Messaging Interchange Specification (AMIS) or Voice Profile for Internet Messaging (VPIM) networking may be necessary. If Cisco Unity will be implemented with dual-switch capability, there are three possible issues to consider:
 - **Legacy voice-mail with IP phones:** Passing Message Waiting Indicator (MWI) information to IP phones may require the use of a Simplified Message Desk Interface (SMDI).
 - **Cisco Unity with traditional telephony:** This arrangement requires the use of the dual-phone system integration, which is described on Cisco.com at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_configuration_guide_chapter09186a0080087f67.html#xtocid1.
 - **Cisco Unity and traditional voice-mail are both deployed:** To exchange voice-mail messages and directory information, AMIS or VPIM must be implemented.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **Circuits for PSTN and PBX connection include analog and digital options. The five interface options are subscriber loop, E & M, T1 or E1 CAS trunking, ISDN with DSS1 signaling, and ISDN with QSIG signaling.**
- **Different types of circuits may be implemented in one location, such as ISDN PRI trunks to the PSTN and QSIG trunks to a PBX.**
- **When choosing a circuit type for an implementation, factors to consider include the existing PBX configuration, line levels in the PBX, and the need for caller ID for services such as billing.**
- **Analog signaling includes loop-start, ground-start, and E&M. E&M is most commonly used for PSTN connections.**
- **Digital signaling is CAS and ISDN. Although it offers many advantages, such as handling more calls at one time.**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0—2-10

Lesson Self-Check Answer key

- Q1) The three summaries should be taken from the following seven common PSTN and PBX circuit options available for deploying on a gateway. The summaries should touch on the following points:
1. Use the subscriber loop when traditional phones connect directly to a voice gateway with an FXS interface.
 2. Use FXO ports for connecting to a CO or PBX.
 3. Use FXS ports to connect to any POTS device such as analog phones, fax machines, and legacy voice-mail systems.
 4. E&M signaling allows extension dialing before the conversation begins and is a simple signaling interface that eliminates glare.
 5. T1/E1 CAS trunks are a common circuit options and exist in many variants that operate over analog and digital interfaces where each channel includes a dedicated signaling element.
 6. Use ISDN with DSS1 signaling so that in addition to the calling-party identification service provided by CAS trunks, supplementary services such as call waiting and do not disturb are available.
 7. ISDN with QSIG signaling is used to interconnect PBXs and to enable supplementary call features between PBXs from different manufacturers.
- Q2) B
- Q3) The following summarizes the four key considerations used to determine PSTN and PBX integration requirement:
1. Top-down or bottom-up integration: The team charged with integrating a PSTN and PBX must build communication strategies to mitigate the issues associated with either a top-down or bottom-up integration approach.
 2. Provisioning specifications: Clocking issues are typical of the problems associated with integrating a PSTN and a PBX. If the service provider equipment does not provide either NT-1 or CSU termination, your organization may have to provide it.
 3. Support of proprietary signaling or connection types: Determine if the gateway needs to support any proprietary signaling or connection types to the PBX.
 4. PBX configuration support: Consider the following issues to ensure that the Cisco voice gateway can be configured to support calls from the legacy PBX:
 - E&M signaling types
 - 2-wire and 4-wire audio implementation
 - Start dial supervision types
 - Dial method types
 - Call progress tones
 - PBX port impedance
- Q4) A
- Q5) The following summarizes the key characteristic of digital circuits:
1. Digital circuits are capable of handling more calls than analog circuits.
 2. Voice signals on digital circuits can be perfectly amplified so distance does not cause signal degradation.
 3. Digital circuits support caller ID, which enables special features such as billing for services used.
 4. Digital circuits using network-side-ISDN PRI enable the access gateway to connect to PBXs and to mimic the behavior of legacy phone switches.
 5. Digital circuits must be synchronized to the same clock source; otherwise, the voice transmission will become garbled. This problem does not exist with analog trunks.

- Q6) The summary should consider the following key considerations:
1. Legacy upgrades: Determine which upgrades to software (for example, upgrading voice cards to the legacy PBX or key system) may be required.
 2. Dial plans: Make modifications to the master dial plan and within the PBX programming to ensure that the legacy system will integrate with the VoIP network.
 3. Trunk reconfiguration: Be prepared to reconfigure the existing trunking or channel configuration.
 4. Voice-mail integration: If legacy voice-mail integration is being considered, AMIS integration may be necessary. Identify if Cisco Unity will be implemented with the dual-switch capability.

Lesson 2

Analog Circuits

Overview

Because many organizations continue to use analog devices, there is still a requirement to integrate analog circuits with VoIP or IP telephony networks.

This lesson describes how to integrate a Cisco voice gateway to the public switched telephone network (PSTN) or a PBX using analog circuits. It starts with a description of the common PSTN and PBX analog gateway signaling interfaces and then describes the common analog call features used on gateways. The lesson continues with a description of the gateway hardware that is required to support analog trunks and a discussion of the available Cisco platforms that provide high-density analog end-station support. It also presents the steps that are needed to configure a gateway to support analog connections and then describes the common analog issues that occur during gateway deployment. The lesson finishes with a description of the troubleshooting tools that are used to resolve analog issues.

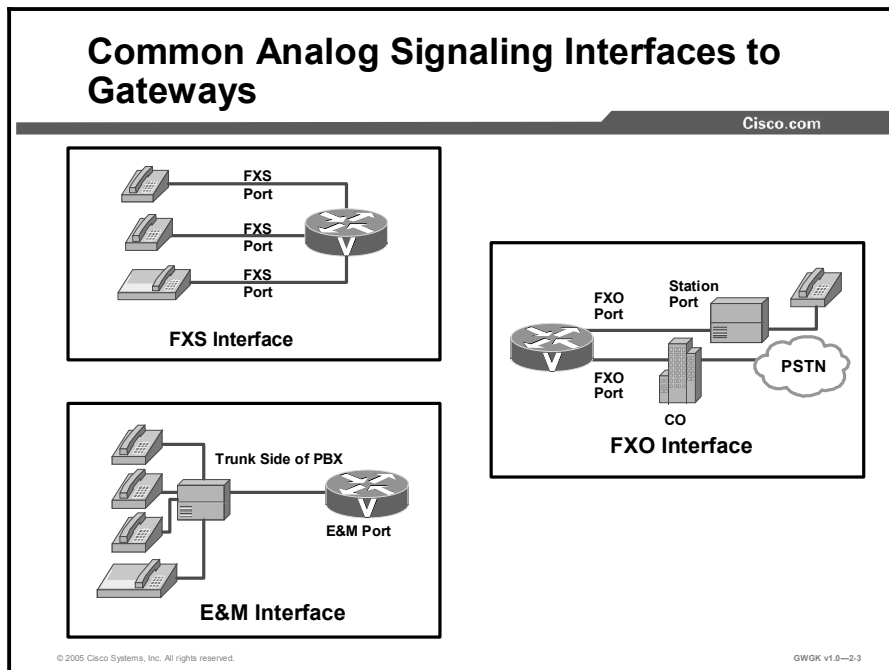
Objectives

Upon completing this lesson, you will be able to integrate a voice gateway into the PSTN or a PBX using analog circuits. This ability includes being able to meet these objectives:

- Describe the common PSTN and PBX analog gateway signaling interfaces
- Describe common analog call features used on gateways
- Describe the gateway hardware required to support analog trunks
- Describe the platforms available to provide high density analog end-station support
- Configure a gateway to support analog connections
- Describe common analog issues that occur during gateway deployment
- Describe the troubleshooting tools that are used to resolve analog issues

Analog Signaling Interfaces

This topic describes the common PSTN and PBX analog gateway signaling interfaces.



To implement a Cisco voice gateway into an analog trunk environment, the Foreign Exchange Station (FXS) interface, the Foreign Exchange Office (FXO) interface, and the receive and transmit (E&M) interface are commonly used.

Analog Call Features

This topic describes the common analog call features that are used on gateways.

Common Analog Call Features

Cisco.com

- **Caller ID**
- **MWI**
- **Call waiting**
- **Caller ID on call waiting**
- **Transfer**
- **Conference**
- **Speed dial**
- **Call forward all**
- **Redial**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0--2.4

PSTN carriers typically offer these analog trunk features that can be supported on home phones. The “Analog Trunk Features” table presents a description of common analog trunk features.

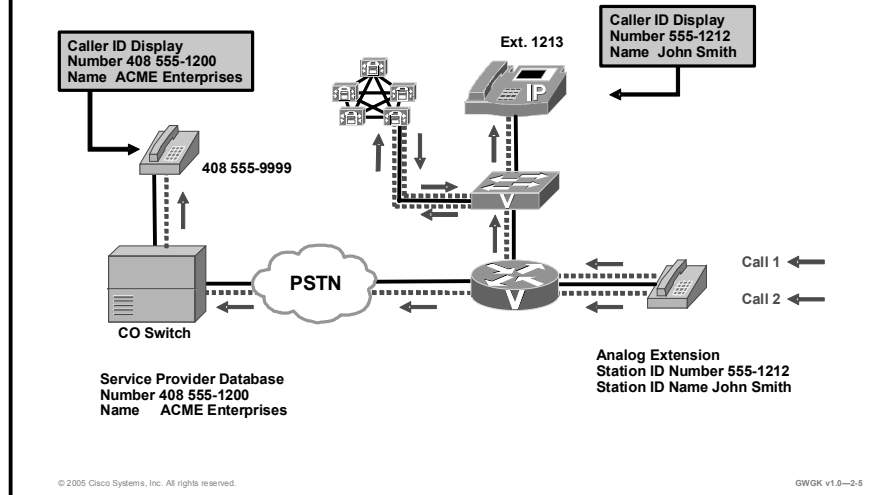
Analog Trunk Features

Feature	Description
Caller ID	Caller ID allows users to see the calling number before answering the phone.
Message-waiting light	There are two methods of analog message-waiting light activation: <ul style="list-style-type: none">■ High-DC voltage (Message-Waiting Indicator [MWI] light) and frequency-shift-key (FSK) messaging■ Stuttered dial tone for phones without a visual indicator These schemes are used by PBX systems and central offices (COs) respectively.
Call waiting	When on a call, and a new call comes in, the user hears an audible tone and can “click over” to the new caller.
Caller ID on call waiting	When on a call, the name of the second caller is announced or the caller ID is shown.
Transfer	This feature includes both blind and supervised transfers using the standard established by Bellcore laboratories. The flash hook method is common with analog trunks.
Conference	Conference calls are initiated from an analog phone using flash hook or feature access codes.

Feature	Description
Speed dial	A user can set up keys for commonly dialed numbers and dial these numbers directly from an analog phone.
Call forward all	Calls can be forwarded to a number within the dial plan.
Redial	A simple last-number redial can be activated from analog phones.

Inbound and Outbound Caller ID with FXO and FXS

Cisco.com



The figure shows a diagram of a small business voice network connected through a gateway to the PSTN. The voice network supports both analog phones and IP phones. The connection to the PSTN is through an FXO port, and the analog phone is connected to the small business network through an FXS port. The issue in this scenario is how the caller ID is passed to call destinations. The following example describes two calls: The first call is to an on-premises destination, and the second call is to an off-premise destination.

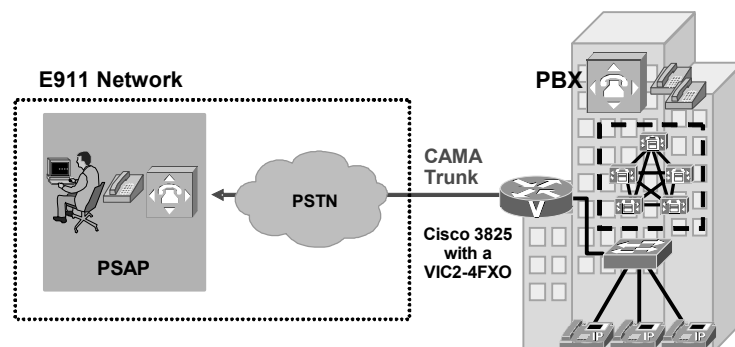
- **Call 1:** Call 1 is from the analog phone to another phone on the premises. The dial peer associated with the FXS port is configured with a station ID name and station ID number. The name is John Smith and the number is 555-0121. When a call is placed from the analog phone to another phone on the premises, an IP phone in this case, the caller name and number are displayed on the screen of the IP phone.
- **Call 2:** Call 2 is placed from the same analog phone, but the destination is off the premises on the PSTN. The FXO port forwards out the station-ID name and station-ID number to the CO switch. The CO switch discards the station ID name and station ID number and replaces them with information that it has configured for this connection.

For inbound calls, caller ID is supported on the FXO port in the gateway. If the gateway is configured for H.323, caller ID is displayed on the IP phones and on the analog phones (if supported).

Note While the gateway supports caller ID, CallManager does not support caller ID on FXO ports if the gateway is configured for Media Gateway Control Protocol (MGCP).

Analog CAMA Trunk Support

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.6

Centralized Automatic Message Accounting (CAMA) interface cards and software configurations are targeted at corporate enterprise networks and at service providers and carriers who are creating new or supplementing existing networks with Enhanced 911 (E911) services. CAMA carries both calling and called numbers by using in-band signaling. This method of carrying identifying information allows the telephone system to send a station identification number to the public safety answering point (PSAP) via multifrequency (MF) signaling through the telephone company E911 equipment. CAMA trunks currently are used in 80 percent of E911 networks. The calling number is needed at the PSAP for two reasons:

- The calling number is used to reference the Automatic Location Identification (ALI) database to find the exact location of the caller and any extra information about the caller that may have been stored in the database.
- The calling number is used as a callback number in case the call is disconnected. A number of U.S. states have initiated legislation that requires enterprises to connect directly to the E911 network. It is expected that the U.S. Federal Communications Commission (FCC) will announce model legislation that extends this requirement to all U.S. states. Enterprises in areas where the PSTN accepts 911 calls on ISDN trunks can use existing Cisco ISDN voice-gateway products because the calling number is an inherent part of ISDN.

The figure shows a Cisco 3825 Voice Gateway with a VIC2-4FXO card connecting an enterprise to an E911 network. Calls to emergency services are routed based on the calling number, not the called number. The calling number is checked against a database of emergency service providers that cross-references the service providers for the caller location. When this information is determined, the call is then routed to the proper PSAP, which dispatches services to the caller location.

During setup of an E911 call, before the audio channel is connected, the calling number is transmitted to each switching point, known as a Selective Router (SR), via CAMA.

The VIC2-2FXO and VIC2-4FXO cards support CAMA via software configuration. CAMA support is also available for the Cisco 2800 Series and 3800 Series Integrated Services Routers (ISRs). It is common for E911 service providers to require CAMA interfaces to their network.

Router Analog Hardware Types

This topic describes the gateway hardware that is required to support analog trunks.

NM and VIC Documentation

Cisco.com

- **High-Density Digital Voice/Fax Network Modules for Cisco 2600XM/2691/2800/3700/3800**
http://www.cisco.com/en/US/products/hw/modules/ps3115/products_data_sheet09186a0080191d41.html
- **NM-HD-1V, NM-HD-2V, and NM-HD-2VE Documentation Roadmap**
http://www.cisco.com/en/US/products/hw/modules/ps5365/products_documentation_roadmap09186a00802c69d5.html
- **NM-HDV-xE1-y and NM-HDV-xT1-y Documentation Roadmap**
http://www.cisco.com/en/US/products/hw/modules/ps2617/products_documentation_roadmap09186a00802c7161.html
- **Voice Hardware Compatibility Matrix (Cisco 17/26/28/36/37/38xx, VG200, Catalyst 4500/4000, Catalyst 6xxx)**
http://www.cisco.com/en/US/products/hw/routers/ps259/products_tech_note09186a00800e73f6.shtml

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0--2.7

The figure presents Cisco source documentation for network modules (NM) and voice interface cards (VICs).

Note For most the current hardware configurations and availability, see the Cisco.com.

Currently, Cisco offers three types of NMs:

- **NM-HDV2:** This NM supports a VIC or voice WAN interface card (VWIC) slot that can be fitted with either digital or analog BRI voice cards or WAN interface cards. This module supports a maximum of 60 channels of digital voice or 4 channels of analog voice in medium codec complexity. This NM must be used with up to four packet voice/data module 2 (PVDM2) packet fax and voice digital signal processor (DSP) modules.
- **NM-HDV2-1T1/E:** This NM includes a built-in T1 or E1 port and a VIC or VWIC slot that can be fitted with either digital or analog voice cards or WAN interface cards. This module supports up to 90 channels of digital voice, or 30 channels of digital voice and 4 channels of analog voice in medium-complexity codec. This module must be used with up to four PVDM2 packet fax or voice DSP modules.
- **NM-HDV2-2T1/E:** This NM includes two built-in T1 or E1 ports and a VIC or VWIC slot that can be fitted with either digital or analog voice cards or WAN interface cards. This module supports up to 120 channels of digital voice, or 60 channels of digital voice and 4 channels of analog voice in medium-complexity codec. This module must be used with up to four PVDM2 packet fax or voice DSP modules.

VICs are daughter cards that slide into the IP communications voice NMs and directly into VIC slots in the Cisco 1700 series, 2800 series, and 3800 series routers. VICs provide the interface to telephony equipment (PBX, key telephone systems, phones, and fax machines) and the PSTN. VICs are important because every branch in an enterprise deployment of IP telephony requires a local connection to the local PSTN for 911 services.

VICs are supported on the NM-1V and NM-2V. VICs denoted by “VIC2” are supported on the NM-HD.

High-Density Analog

This topic describes the platforms that are available to provide high-density analog end-station support.



The figure shows the Cisco VG224 Analog Phone Gateway and the Cisco VG248 Analog Phone Gateway. The Cisco VG224 Analog Phone Gateway offers Cisco IOS software manageability with 24 analog phone lines that can be used as extensions to the Cisco CallManager system. The VG224 Analog Phone Gateway is ideal for implementations in which analog phones are needed. At locations with MGCP fallback, the VG224 Analog Phone Gateway provides a high level of availability and ease of manageability using Cisco IOS software monitoring features. The Cisco VG248 Analog Phone Gateway offers 48 fully featured analog phone lines in a 19-inch rack-mount chassis that can be used as extensions to the Cisco CallManager system. The Cisco VG248 Analog Phone Gateway is ideal for implementations where it is necessary to use analog phones because it provides a high level of functionality at those locations.

VG248 and VG224 Analog Feature Support

Cisco.com

Analog Feature	VG224 (MGCP)	VG224 (SCCP)	VG248 (SCCP)
Cisco IOS software-based platform	Yes	Yes	No
# FXS ports	24	24	48
Basic call (with Cisco CallManager configuration)	X	X	X
Modem pass-through	X	H.323/MGCP	X
Fax (T.38, Cisco FR, Pass-through)	X	H.323/MGCP	X T.38 gateway controlled
Caller ID	X	X	X
MWI (stutter)		X	X
Call waiting		X	X
Hook flash transfer		X	X
Conference		X	X
Feature access code		X	X
Redial		X	X
Call forward all		X	X
Speed dial		X	X

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—2.9

The Cisco VG224 Analog Phone Gateway and the Cisco VG248 Analog Phone Gateway support a number of analog features. The table in the figure describes the support for common analog features by the Cisco VG224 Analog Phone Gateway and the Cisco VG248 Analog Phone Gateway. Currently, the VG224 Analog Phone Gateway supports MGCP and the Skinny Call Control Protocol (SCCP).

Note There are numerous options for configuring the VG224 Analog Phone Gateway and VG248 Analog Phone Gateway. For analog support, be sure to check Cisco.com for current configuration options.

Common Analog Supplementary Call Features

Cisco.com

	VG 224 (MGCP)	VG 224 (SCCP)	VG248 (SCCP)	Cisco CallManager
Out-going caller ID	X	X	X	X
In-coming caller ID	X	Service provider	Service provider	X
MWI (light and stutter dial tone)		X	X	
Call waiting		X	X	
Caller ID on call waiting			X	
Hook flash transfer		X	X	Service provider
Conference		X	X	Service provider
Speed dial			X	
Call forward all			X	
Redial			X	

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—2-10

The different supplementary call features that are available for each voice gateway are presented in the table in the figure and associate with the control protocol running on the gateway, not the gateway hardware. In general, FXS ports controlled by H.323, MGCP, and session initiation protocol (SIP) support only basic call features. SCCP-controlled ports support the supplementary call features, and these depend on which protocol the gateway supports (or is configured for) on its FXS ports.

Until recently, the Cisco VG248 Analog Phone Gateway was the only Cisco SCCP-controlled FXS gateway. Cisco IOS gateways supported only H.323, MGCP, and SIP. Now, the Cisco VG224 Analog Phone Gateway with SCCP control has been introduced, and soon Cisco IOS gateways will include supplementary call features. Basic and supplementary call features are software dependent, not hardware dependent.

Basic call features are designed for fax machines, lobby phones, emergency backup phones, and hallway phones. The basic call features supported by H.323, MGCP, and SIP are dial tone, dual tone multifrequency (DTMF) dialing to originate a call, ringing, call answer, fax and modem relay, fax pass-through, and caller ID.

The figure shows which supplementary call features are supported by gateways configured with MGCP and SCCP control protocols. The “Service provider” entry in the table means that the supplementary call feature is only available if the service provider supplies this feature. Supplementary call features are typical of those found on desktop phones.

Cisco CallManager Express Feature Availability with VG224

Cisco.com

Analog Feature	VG224 (H.323)	VG224 (SIP)	VG224 (SCCP)
Basic call (with Cisco CallManager configuration)	X	X	X
Modem Pass-through	X	X	H.323/MGCP
Fax (T.38, Cisco FR, Pass-through)	X	X	H.323/MGCP
Caller ID	Via script	Via script	X
MWI (stutter/visual)		Via script	X
Call waiting	Via script	Via script	X
Hook flash transfer	Via script	Via script	X
Conference			X
Feature access code			X
Redial	Phone Function	Phone Function	X
Call forward all			X
Speed dial			X
SMDI			X

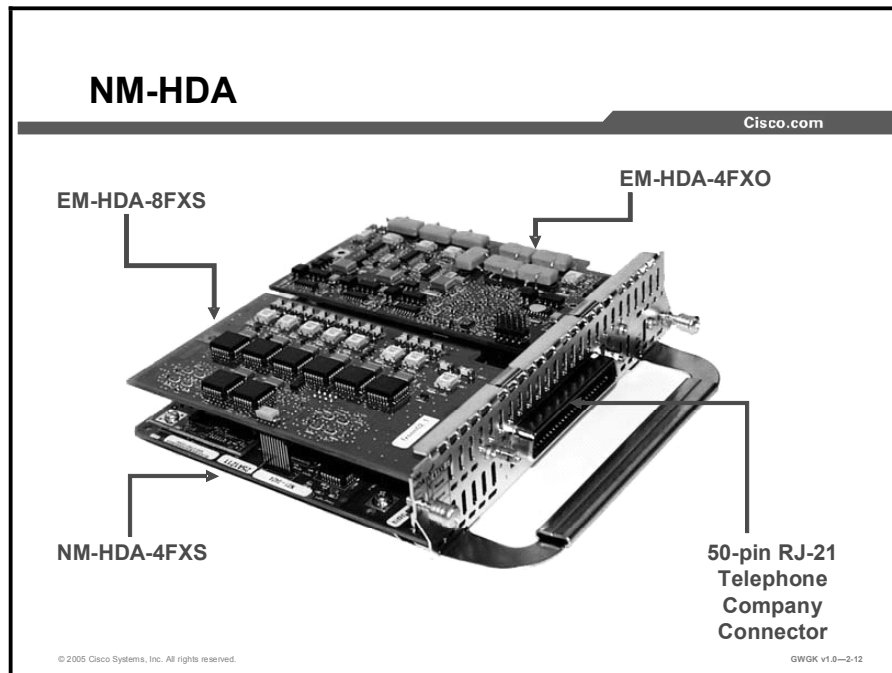
• VG248 not supported with CallManager Express

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.11

The Cisco VG224 Analog Phone Gateway supports a number of analog features that are supported by Cisco CallManager Express. The table in the figure describes these features.

Note The VG248 Analog Phone Gateway is not supported by Cisco CallManager Express.

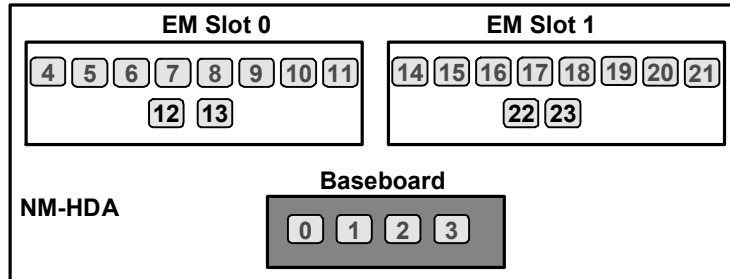


The figure shows a picture of the Cisco high density analog (HDA) NM (NM-HDA). The NM-HDA baseboard shown is the NM-HDA-4FXS. The two port expansion modules (EMs) are populated with an EM-HDA-8FXS and an EM-HDA-4FXO. The NM-HDA shown also has a 50-pin RJ-21 telephone company connector. Ports from the modules (base and expansion) are mapped to specific pins. There is also an optional DSP-HDA-16 DSP module that plugs onto the NM-HDA baseboard.

Note A configuration using two 8-port FXS EMs is not supported.

Port Numbering on the NM-HDA

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-13

The “NM-HDA Port Number” table provides details on the NM-HDA ports.

NM-HDA Port Numbering

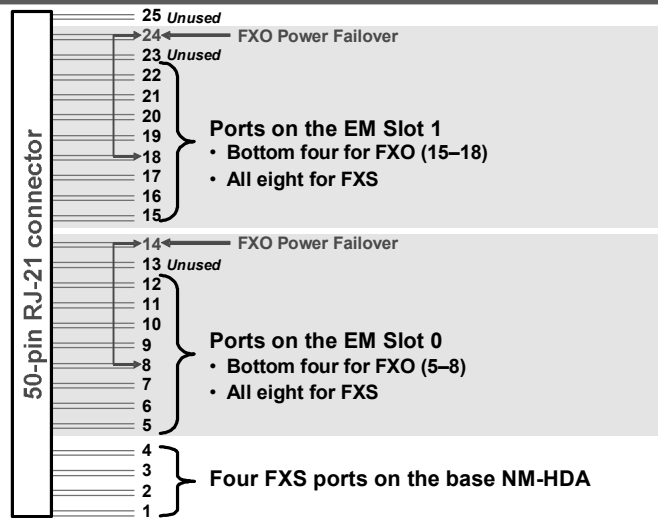
Component	Number of Ports	Mapped to These Port Numbers
Baseboard	four	x/0/0 – x/0/3
EM in Slot 0	eight	x/0/4 – x/0/11
EM in Slot 1	eight	x/0/14 – x/0/21

When configuring the NM-HDA, consider the following:

- Although 24 port numbers are possible, a maximum of 16 active ports are supported on the NM-HDA.
- The middle digit of the port number for the NM-HDA is always 0.
- EM slots have 10 port numbers allocated to them, but only the bottom 8 can be used.

RJ-21 Pinouts on the NM-HDA

Cisco.com



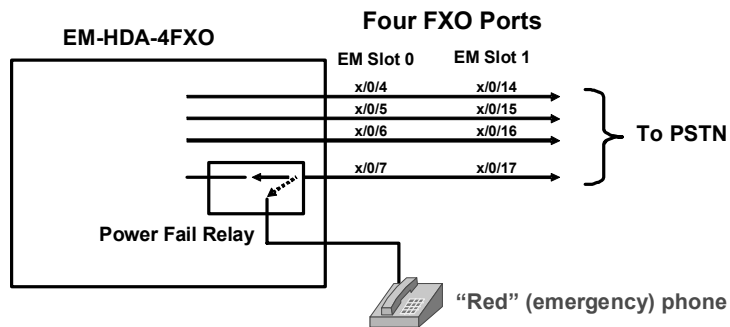
© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.14

The figure shows the 50-pin RJ-21 connector pin that maps to the port numbers on the NM-HDA. The numbers 1 to 25 are the pin numbers for the RJ-21 connector.

NM-HDA FXO Power Failover

Cisco.com



The solid arrow in the "Power Fail Relay" box indicates a disconnected state and represents the default condition.

© 2005 Cisco Systems, Inc. All rights reserved.

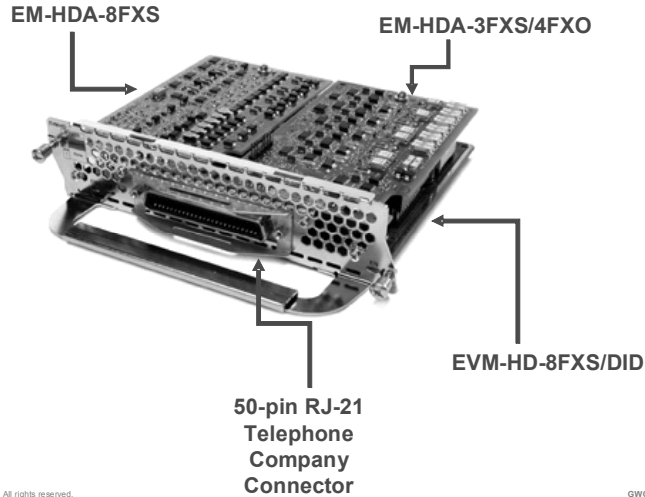
GWGK v1.0-2-15

The figure shows a schematic of a NM-HDA with the four FXO ports that are connected to the PSTN. The "Red" phone is normally disconnected; but during power failure, it has a direct metallic path to the PSTN via a relay on the EM-HDA-4FXO. In the figure, the ports x/0/7 and x/0/17 failover, via the power fail relay, to a phone that is connected to the EM-HDA.

Note The numbers in this figure, x/0/4 to x/0/17, are the identification for the ports on the EM-HDA.

EVM-HD Hardware

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.16

The figure shows a picture of the Cisco NM-HDA and Digital Extension Module for Voice and Fax (EVM-HD). The baseboard shown is the EVM-HD-8FXS/DID. The DID in the product name stands for Direct Inward Dialing. The two port EMs are populated with an EM-HDA-8FXS and an EM-HDA-3FXS/4FXO. The EVM-HD shown also has a 50-pin RJ-21 telephone company connector.

RJ-21 Pinouts on the EVM-HD

Cisco.com

Tip and Ring	EM-HDA-6FXO	EM-HDA-8FXS	EM-HDA-3FXS/4FXO	
24 / 49	Power Fail	FXS 2/0/23	FXO 2/0/23	Ports on EM Slot 1
23 / 48	Unused	FXS 2/0/22	FXO 2/0/22	
22 / 47	FXO 2/0/21	FXS 2/0/21	FXO 2/0/21	
21 / 46	FXO 2/0/20	FXS 2/0/20	FXO 2/0/20	
20 / 45	FXO 2/0/19	FXS 2/0/19	Unused	
19 / 44	FXO 2/0/18	FXS 2/0/18	FXS 2/0/18	
18 / 43	FXO 2/0/17	FXS 2/0/17	FXS 2/0/17	
17 / 42	FXO 2/0/16	FXS 2/0/16	FXS 2/0/16	
16 / 41	Power Fail	FXS 2/0/15	FXO 2/0/15	
15 / 40	Unused	FXS 2/0/14	FXO 2/0/14	
14 / 39	FXO 2/0/13	FXS 2/0/13	FXO 2/0/13	Ports on EM Slot 0
13 / 38	FXO 2/0/12	FXS 2/0/12	FXO 2/0/12	
12 / 37	FXO 2/0/11	FXS 2/0/11	Unused	
11 / 36	FXO 2/0/10	FXS 2/0/10	FXS 2/0/10	
10 / 35	FXO 2/0/9	FXS 2/0/9	FXS 2/0/9	
9 / 34	FXO 2/0/8	FXS 2/0/8	FXS 2/0/8	
8 / 33	FXS 2/0/7			
7 / 32	FXS 2/0/6			
6 / 31	FXS 2/0/5			
5 / 30	FXS 2/0/4			
4 / 29	FXS 2/0/3			
3 / 28	FXS 2/0/2			
2 / 27	FXS 2/0/1			
1 / 26	FXS 2/0/0			

Eight FXS/DID baseboard ports

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.17

The figure shows the 50-pin RJ-21 telephone company connector receive and transmit pin mapping to the port numbers on the EVM-HD.

EVM-HD Configuration Options

Cisco.com

Baseboard	EM Slot 0	EM Slot 1	FXS or DID	FXS	FXO	Module
EVM-HD-8FXS/DID			8			8
	EM-HDA-8FXS		8	8		16
	EM-HDA-8FXS	EM-HDA-8FXS	8	16		24
	EM-HDA-8FXS	EM-HDA-3FXS/4FXO	8	11	4	23
	EM-HDA-8FXS	EM-HDA-6FXO	8	8	6	22
	EM-HDA-8FXS	EM-4BRI-NT/TE	8	8		24
	EM-HDA-3FXS/4FXO		8	3	4	15
	EM-HDA-3FXS/4FXO	EM-HDA-3FXS/4FXO	8	6	8	22
	EM-HDA-3FXS/4FXO	EM-HDA-6FXO	8	3	10	21
	EM-HDA-3FXS/4FXO	EM-4BRI-NT/TE	8	3	4	23
	EM-HDA-6FXO		8		6	14
	EM-HDA-6FXO	EM-HDA-6FXO	8		12	20
	EM-HDA-6FXO	EM-4BRI-NT/TE	8		6	22
	EM-4BRI-NT/TE		8			16
	EM-4BRI-NT/TE	EM-4BRI-NT/TE	8			24

© 2005 Cisco Systems, Inc. All rights reserved.

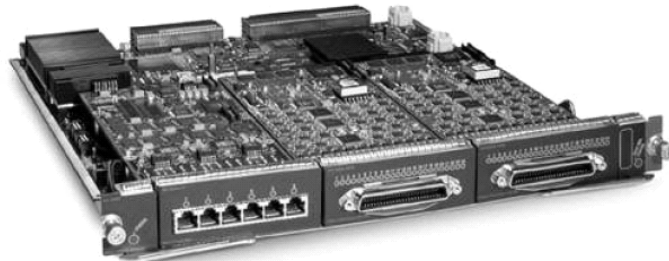
GWGK v1.0-2-18

The figure shows the current configuration options for the EVM-HD.

Note BRI information has been removed to focus on the analog configuration options.

Cisco CMM for the Cisco Catalyst 6000

Cisco.com



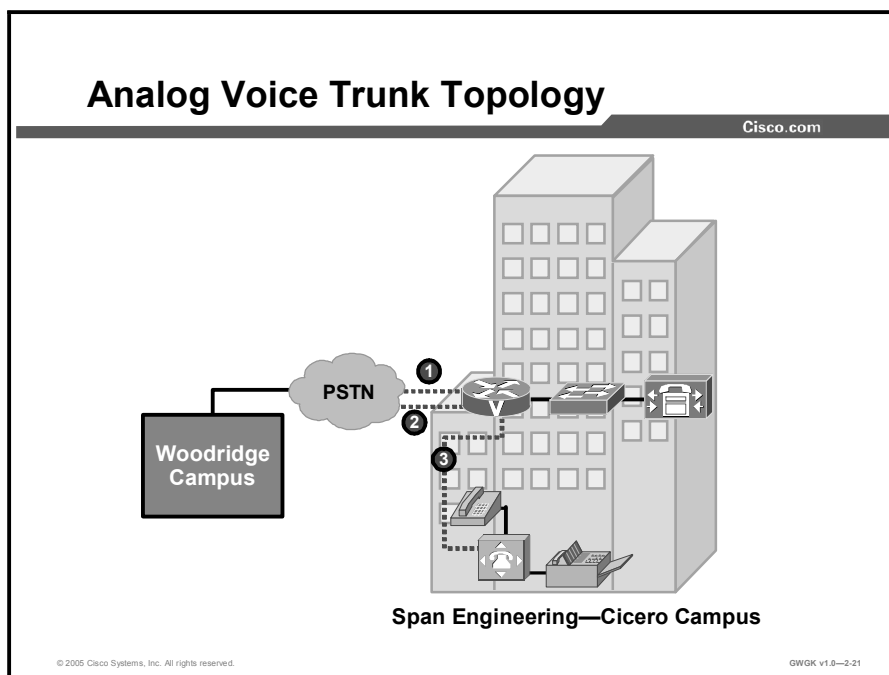
© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-2.19

The figure shows the Cisco Communication Media Module (CMM). The Cisco CMM introduces a new modular line card in the Cisco Catalyst 6500 Series switches and the Cisco 7600 Series routers. The Cisco CMM supports four different types of port adapters including 6-port T1, 6-port E1, 24-port FXS, and 128-port conferencing and transcoding port adapters. Up to four port adapters can be installed on a single CMM line card. Customers have the flexibility of mixing any of the four types of port adapters in a single CMM; however, one slot is internal and can only accommodate the DSP module.

Analog Trunk Configuration

This topic describes how to configure a gateway to support analog connections.



The figure shows a simplified analog voice topology. The “Line Description” table provides the key to the dotted lines in the figure.

Line Description

Line Number	Description
1	an FXO trunk to the PSTN
2	a CAMA trunk to the E911 system
3	an E&M trunk to the PBX

Example: Analog FXO Voice Trunk Configuration

Cisco.com

```
hostname router Cicero

! Configure pots dial-peer 1
dial-peer voice 1 pots
destination-pattern 1801.....
port 0/0
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-2.22

The figure shows an analog FXO voice trunk configuration example. To configure a dial peer, point to the FXO voice port. Under most circumstances, the default voice-port values are sufficient for configuring an FXO port to transport voice. However, if caller ID is required, that feature must be specifically configured.

Configuring FXS and FXO Caller ID

Cisco.com

- **Step 1: Enable caller ID**
- **Step 2: Configure the station name on FXS voice ports connected to user telephone sets.**
- **Step 3: Configure the station number on FXS voice ports connected to user telephone sets.**
- **Step 4: (Optional) Block display of the calling party information on terminating FXS ports.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.23

The “Configuring FXS and FXO Voice Ports” table provides details on the steps required to configure FXS and FXO voice ports to support caller ID.

Configuring FXS and FXO Voice Ports

Step	Action	Notes
1.	<code>Router(config)# caller-id enable</code>	<p>Use this command to enable caller ID. This command applies to FXS voice ports that send caller ID information and to FXO ports that receive caller ID information. By default, caller ID is disabled.</p> <p>To disable the sending or receiving of caller ID information, use the no form of this command.</p> <p>If the station-id or a caller-id alerting command is configured on the voice port, these commands automatically enable caller ID, and the caller-id enable command is not necessary.</p>
2.	<code>Router(config-voiceport)# station-id name name</code>	<p>Use this command to configure the station name on FXS voice ports connected to user telephone sets. This sets the caller ID information for on-net calls originated by the FXS port. You can also configure the station name on an FXO port of a router where incoming caller ID information from the PSTN subscriber line is expected. In this case, if no caller ID information is included on the incoming PSTN call, the called party receives the information configured on the FXO port instead. If the PSTN subscriber line does provide caller ID information, this information is used and the configured station name is ignored.</p> <p>The <i>name</i> argument is a character string of 1 to 15 characters identifying the station.</p> <p>This command applies only to caller ID calls, not to automatic number identification (ANI) calls. ANI supplies calling number identification only.</p>

Step	Action	Notes
3.	Router (config-voiceport) # station-id number number	<p>Use this command to configure the station number on FXS voice ports connected to user telephone sets. This command sets the caller ID information for on-net calls originated by the FXS port.</p> <p>You can also configure the station number on an FXO port of a router for which incoming caller ID information from the PSTN subscriber line is expected. In this case, if no caller ID information is included on the incoming PSTN call, the called party receives the information configured on the FXO port instead. If the PSTN subscriber line does provide caller ID information, this information is used and the configured station name is ignored.</p> <p>If the caller ID station number is not provided by either the incoming PSTN caller ID or by the station number configuration, the calling number included with the on-net routed call is determined by Cisco IOS software using a reverse dial-peer search. In this case, the number is obtained by searching for a POTS dial peer that refers to the voice-port and the destination-pattern number from the dial peer that is used.</p> <p>The <i>number</i> argument is a string of 1 to 15 characters identifying the station telephone or extension number.</p> <p>To remove the number, use the no form of this command.</p>
4.	Router(config-voiceport)# caller-id block	<p>Use this command to block a display of the calling party information on terminating FXS ports.</p> <p>(FXS ports only.) When this command is configured at the originating end of a call, it requests that the originating calling party information not be displayed at the called party telephone.</p> <p>The calling party information is included in the routed on-net call because this is often required for other purposes, such as billing and call blocking. The request to block a display of the calling party information on terminating FXS ports is normally accepted by Cisco routers, but no guarantee can be made regarding the treatment by other equipment.</p> <p>This command affects all calls sent to an FXO station from the configured FXS station. The CO may supply a feature code that a user can dial to block caller ID transmission on a call-by-call basis.</p> <p>When a blocked-information call passes through an FXO interface on the way to its destination, the blocking is passed on to the receiving party.</p> <p>To allow the display of caller ID information, use the no form of this command.</p>
5.	Router (config-voiceport) # no shut	<p>Use the following command to enable CAMA signaling.</p> <p>You must perform the shut and no shut commands in Steps 3 and 4 to complete the activation of CAMA on the voice ports that are being configured.</p>

Example: Analog FXO Voice Trunk Configuration

Cisco.com

```
Router> show voice port 1/1/1
FXS 1/1 Slot is 1, Port is 1
Type of VoicePort is FXS
Operation State is UP
Administrative State is UP
...

Caller ID Info Follows:
Standard BELLCORE
Station name A. Person, Station number 4085551111
Caller ID presentation unblocked
Output attenuation is set to 14 dB
Caller ID is transmitted after 1 rings
...
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—2.24

The figure shows a sample analog FXO voice trunk configuration on a Cisco router. The first highlighted section identifies the voice port as an FXS port. The second highlighted section shows that the FXS port is configured with a Bellcore/Telcordia standard, (the *cptone* value is *northamerica*), a station name, and a station number. The caller ID alerting ring setting is 1.

Note For more details on configuring *cptone* and the caller ID-alerting ring, refer to *Cisco IOS Voice, Video, and Fax Configuration Guide Release 12.2, Appendix B - Caller ID* at http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7df.html#1049232.

Configuring Analog CAMA Trunks

Cisco.com

- **Step 1: Identify the voice port to be configured.**
- **Step 2: Select the desired signal and specify the type of CAMA signaling.**
- **Step 3: Build the table that translates the NPA or area code into a single MF digit.**
- **Step 4: Disable the selected port on the voice interface card.**
- **Step 5: Enable CAMA signaling.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-3.25

To configure the Cisco VIC2-2FXO or VIC2-4FXO cards to recognize CAMA signaling, perform the steps detailed in the “Configuring Analog CAMA Trunks” table.

Note When a port on these VICs is not configured for CAMA signaling, the port functions as a normal FXO port, and all existing FXO functionality is available.

Configuring Analog CAMA Trunks

Step	Action	Notes
1.	Router(config)# voice-port slot/port	<p>Use this command to identify the voice port to be configured.</p> <p><i>slot</i>: This is the slot in the router in which the VIC is installed. The only valid entry is 1.</p> <p><i>port</i>: This is the voice port number. Valid values are as follows:</p> <ul style="list-style-type: none">■ T1: ANSI T1.403 (1989), Bellcore TR-54016■ E1: ITU G.703■ Analog voice: Up to six ports (FXS, FXO, E&M)■ Digital voice: Single T1/E1 with cross-connect drop and insert, CAS and CCS signaling, PRI QSIG■ Ethernet: Single 10BASE-T■ Serial: Two five-in-one synchronous serial ports (ANSI EIA/TA-530, EIA/TA-232, EIA/TA-449; ITU V.35, X.21, Binary Synchronous Communication Protocol [bisync], polled async)

Step	Action	Notes
2.	<pre>Router(config-voiceport)# signal {cama {KP-0-NPA-NXX- XXXX-ST KP-0-NXX-XXXX-ST KP-2-ST KP-NPD-NXX-XXXX-ST} groundstart loopstart}}</pre>	<p>Use this command to select the desired signal and to specify the type of CAMA signaling.</p> <p>There are four CAMA signaling options for transmitting the calling number:</p> <ul style="list-style-type: none"> ■ Type 1: The KP-0-NXX-XXXX-ST option ■ Type 2: The KP-0-NPA-NXX-XXXX-ST option, which is common ■ Type 3: The KP-2-ST option ■ Type 4: The KP-NPD-NXX-XXXX-ST option <p>The card default, without CAMA enabled, is loopstart.</p> <p>To reset to the default, use the no form of this command.</p>
3.	<pre>Router(config-voiceport)# ani mapping NPD-value NPA-number</pre>	<p>Use this command to build the table that translates the Numbering Plan Area (NPA), or area code, into a single MF digit. The number of Numbering Plan Digits (NPDs) that are programmed is determined by local policy and by the number of NPAs or area codes that the PSAP serves.</p> <p>The NPD value range is 0 to 3.</p> <p>The NPA number range is 100 to 999. To disable ANI mapping, use the no form of this command.</p>
4.	<pre>Router(config-voiceport)# shut</pre>	<p>Use this command to disable the selected port on the VIC.</p> <p>Repeat Step 4 until all NPAs (area codes) are configured or until the NPD range maximum is reached.</p>
5.	<pre>Router(config-voiceport)# no shut</pre>	<p>Use this command to enable CAMA signaling.</p> <p>You must perform the shut and no shut commands in Steps 3 and 4 to complete the activation of CAMA on the voice ports you are configuring.</p>

The CAMA signaling options that are typically provided by the PSAP are as follows:

- **KP-0-NXX-XXXX-ST:** This option is used for a 7-digit ANI transmission. The NPA or area code is implied by the trunk group and is not transmitted.
- **KP-0-NPA-NXX-XXXX-ST:** This option is used for a 10-digit transmission. The E.164 number is fully transmitted.
- **KP-2-ST:** This is the default transmission when the CAMA trunk cannot obtain a corresponding NPD in the look-up table, or when the calling number is fewer than 10 digits (NPA digits are not available).
- **KP-NPD-NXX-XXXX-ST:** This is the option used for an 8-digit ANI transmission in which the NPD is a single MF digit that is expanded into the NPA. The NPD table is preprogrammed by configuring ANI mapping in the sending and receiving equipment (on each end of the MF trunk); for example: 0 = 408, 1 = 510, 2 = 650, 3 = 415.
 - NPD values range from 0 to 3. Examples of telephone numbers in this signaling option are:
 - 05550123 = (408) 555-0123
 - 25550199 = (650) 555-0199

Note If the NPD value does not match a value in the NPD table, the CAMA signaling option defaults to KP-2-ST.

For information on configuring CAMA, see *FXO, FXS, and E&M VIC Support on Cisco 1700 Series Routers* at http://www.cisco.com/en/US/products/hw/routers/ps221/prod_configuration_guide09186a008019b16e.html.

Example: Analog CAMA Trunk Configuration

Cisco.com

```
voice-port 0/0
  ani mapping 0 408
  ani mapping 1 510
  ani mapping 2 650
  ani mapping 3 415
  signal cama KP-NPD-NXX-XXXX-ST
  shut
no shut
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.28

The following example shows the configuration of the VIC2-2FXO card for eight-digit transmission. In this example, ANI mapping is shown for the following NPAs: 0 = 408, 1 = 510, 2 = 650, 3 = 415.

You can verify the configuration by using the **show run** command, the **show voice port** command, or the **show voice port summary** command. The following is an example output that confirms the configuration depicted in the figure. After running a **show voice port** command, the following commands help to verify a successful analog CAMA trunk configuration:

```
router # show run
!
voice-port 0/0
  ani mapping 0 408
  ani mapping 1 510
  ani mapping 2 650
  ani mapping 3 415
  signal cama KP-NPD-NXX-XXXX-ST
!
end
```

The following example shows the result of a **show voice port summary** command on a router with a VIC2-2FXO card in slot 0. Port 0 is configured for CAMA, and port 1 is configured for normal FXO operation.

```
router# show voice port summary
-----
PORT      CH  SIG-TYPE  ADMIN OPER STATUS  STATUS  EC
===== ==  =====  =====  =====  =====  =====  ==
0/0      --  fxo-cama  up    up    idle    on-hook  y
0/1      --  fxo-ls   up    up    idle    on-hook  y
```


Analog E&M Trunk Configuration

Cisco.com

- **Step 1:** Enter the global configuration mode.
- **Step 2:** Identify the voice port you want to configure and enter the voice port configuration mode.
- **Step 3:** Select the appropriate signal type for this interface.
- **Step 4:** Select the appropriate cabling scheme for this voice port.
- **Step 5:** Select the appropriate E&M interface type.

```
!Configure pots dial-peer 1
dial-peer voice 1 pots
destination-pattern 1408555....
port 0/0

!Configure the E&M interface
voice-port 0/0
signal immediate
operation 4-wire
type 2
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-2.27

The figure shows a sample E&M configuration and the sequence of commands needed to configure a basic E&M trunk. Unlike FXS and FXO voice ports, the default E&M voice-port parameters are not sufficient to enable voice and data transmission over your IP network. Because of the inherent complexities of PBX networks, E&M voice-port values must match those specified by the particular PBX device to which it is connected.

To configure E&M voice ports, use the commands presented in the “Configuring an E&M Trunk” table. Enter the commands beginning in privileged EXEC mode.

Configuring an E&M Trunk

Step	Action	Notes
1.	<code>configure terminal</code>	Use this command to enter the global configuration mode.
2.	<code>voice-port slot-number/port</code>	Use this command to identify the voice port you want to configure and to enter the voice-port configuration mode.
3.	<code>signal {wink-start immediate delay-dial}</code>	Use this command to select the appropriate signal type for this interface.
4.	<code>operation {2-wire 4-wire}</code>	Use this command to select the appropriate cabling scheme for this voice port.

Step	Action	Notes
5.	type {1 2 3 5}	<p>Use this command to select the appropriate E&M interface type.</p> <p>type 1 is for the following lead configuration:</p> <ul style="list-style-type: none"> ■ E: output, relay to ground ■ M: input, referenced to ground <p>type 2 is for the following lead configuration:</p> <ul style="list-style-type: none"> ■ E: output, relay to signal ground (SG) ■ M: input, referenced to ground ■ Signal battery (SB): feed for M, connected to –48V ■ SG: return for E, galvanically isolated from ground <p>type 3 is for the following lead configuration:</p> <ul style="list-style-type: none"> ■ E: output, relay to ground ■ M: input, referenced to ground ■ SB: connected to –48V ■ SG: connected to ground <p>type 5 is for the following lead configuration:</p> <ul style="list-style-type: none"> ■ E: output, relay to ground ■ M: input, referenced to –48V

Common Analog Issues

This topic describes some common analog issues that occur during gateway deployment.

Common Analog Issues

Cisco.com

- **Impedance mismatch**
- **Voice volume**
- **Cabling and port programming**
- **FXO disconnect**
- **Caller ID**
 - **FXS based**
 - **FXO based**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-2.29

The following describes some common analog issues that occur during gateway deployment:

- **Impedance mismatch:** If the impedance is set incorrectly (there is an impedance mismatch), a significant amount of echo is generated. In addition, gains, or the charge in the circuit due to signal input, might not work if there is an impedance mismatch.

Note This echo can be masked if the **echo-cancel** command has been enabled.

- **Voice volume:** Incorrect input or output levels can cause echo, as can an impedance mismatch. Too much input gain can cause clipped or fuzzy voice quality. If the output level is too high at the remote router voice port, the local caller hears echo. If the local router voice-port input decibel level is too high, the remote side hears clipping. If the local router voice port input decibel level is too low, or the remote router output level is too low, the remote side voice can be distorted at a very low volume and DTMF may be missed.
- **Cabling and port programming:** The majority of faults with E&M ports are due to incorrect wiring or PBX port programming.

- **FXO disconnect:** A switch used in PBX and PSTN key systems requires that a user hang up the phone when the call is terminated. Human intervention is not built into the router FXO port. The FXO port expects the switch to indicate when to hang up. Consequently, it is not guaranteed that a near-end or far-end FXO port will disconnect the call after either end of the call has hung up. There are two problems associated with the inability for a near-end or far-end FXO port to disconnect: Charges for the line could be billed to the customer and all the channels on the trunk will eventually become blocked. The following describes how disconnect supervision and its counterpart answer supervision have been created to handle these problems:
 - **Disconnect supervision:** PBX and PSTN switches use several different methods to indicate that a call should be disconnected because one or both parties have hung up. The following commands are used to configure the router to recognize the type of signaling in use by the PBX or PSTN switch connected to the voice port:
 - **Battery reversal disconnect:** When the **battery reversal disconnect** command is enabled on the voice port, changes in the polarity of the line-in generated by the connected switch indicate that the line-in has been disconnected. Changes in the line-in polarity indicate changes in call state such as off-hook or call disconnect. The **battery reversal disconnect** command is enabled by default when the **disconnect supervision** command is enabled.
 - **Battery denial disconnect:** When the **battery denial disconnect** command is enabled on the voice port, short (approximately 600 ms) interruption of line power to indicate that the line-in has been disconnected. The **battery denial disconnect** command is enabled by default when the **disconnect supervision** command is enabled.
 - **Supervisory tone disconnect (STD):** STD occurs when the connected switch provides a special tone to indicate a change in the call state. Some PBXs and PSTN CO switches provide a 600-ms interruption of line power as a supervisory disconnect, and others provide STD. This is the signal that the router is looking for when the no supervisory disconnect command is configured on the voice port.
 - **FXO STD:** If the FXO STD is configured and a detectable tone from the PSTN or PBX is detected by the DSP, the analog FXO port goes on-hook. This feature prevents an analog FXO port from remaining in an off-hook state after an incoming call is ended. The FXO supervisory disconnect tone enables interoperability with PSTN and PBX systems whether or not they transmit supervisory tones.

Note This feature applies to analog FXO ports with loop-start signaling. This feature is found on the Cisco 2600 Series, the Cisco 3600 Series, and Cisco 2800 ISR Series routers.

- To configure a voice port to detect incoming tones, you must know the parameters of the tones expected from the PBX or PSTN. Then create a voice class that defines the tone-detection parameters and apply the voice class to the applicable analog FXO voice ports. This procedure configures the voice port to go on-hook when it detects the specified tones. The parameters of the tones need to be precisely specified to prevent unwanted disconnects due to the detection of nonsupervisory tones or noise.

- An STD is normally a dual tone with two frequencies; however, tones of only one frequency can also be detected. Use caution if you configure voice ports to detect nondual tones because unwanted disconnects can result from detection of random tone frequencies. You can configure a voice port to detect a tone with one on/off time cycle, or you can configure it to detect tones in a cadence pattern with up to four on/off time cycles.
- **FXS-based caller ID:** If you have caller ID problems on telephones connected to FXS ports, the following tips may be helpful:
 - Try a different brand of phone to confirm that the problem is not caused by a malfunctioning or incompatible caller ID telephone.
 - Ensure that the **cptone** command is set correctly to reflect your locale.
 - If the call time display is incorrect, check the router clock setting. A Network Time Protocol (NTP) server is recommended for accurate display of the local time.
 - If expected information is not displayed, use the **show call history** command to make sure that the information that the router received during the call setup is complete.
 - The line voltage available on the FXS voice ports of the Cisco 2600 and 3600 series routers is -24V. Some phones do not recognize -24V caller ID signaling.
- **FXO-based caller ID:** If you have caller ID display problems on FXO ports, the following tips may be helpful:
 - Disconnect the router from the phone line and attach a caller-ID-equipped telephone to verify that the CO is sending caller ID information:
 - Listen and watch to see when the caller ID information is displayed—before the first ring, after the first ring, or after the second ring.
 - Make sure that the router configuration matches the timing of the display. If the phone is answered during the first ring, does this cause the phone not to display the caller ID information? If so, the CO may be sending the caller ID information after the first ring, requiring a change to a caller ID alerting setting. Make sure that the router is not configured to answer the call on the FXO before the caller ID information is received. If needed, increase the number of rings required before answering.
 - Use the **show call history** command to check the information received by the caller ID unit.

Common Symptoms of Analog Issues

Cisco.com

- In Cisco CallManager, the analog FXO and FXS card is not recognized by the gateway.
- In Cisco CallManager the FXO card does not send or pulse out digits.
- The phone continues to ring on an FXO or FXS network after the user hangs up.
- No dial tone is received from gateway voice port after the phone goes off-hook.
- The second FXS port shuts down when a call is placed on the first port.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.28

There are several common analog issues that occur when you are connecting an analog system to a gateway. Five of the most common issues and their possible solutions are as follows:

- **Using Cisco CallManager, the analog FXO and FXS card is not recognized by the gateway.** The solution to this problem involves the following procedure:
 1. Issue the **show version** command on the router to determine if the hardware is installed on the router module.
 2. Issue the **show diag** command. If this command does not clearly specify the name of this module and instead lists “Unknown module” or “Unknown card”, ensure that you have the correct Cisco IOS software features. You must have the “Plus” feature set installed, which is noted by the “-s” in the Flash file name.
 3. If you have the correct features installed and still cannot see the module, make sure the module is seated properly in the slot. To make certain, save your configuration, turn off the router, and reseal the VIC in the network module (if it applies to your platform) and then reseal the module (VIC or NM-2V) in the router slot. Restart the router, and when the orange lights disappear, see if you can identify the hardware correctly.
 4. To test an FXS port, connect an analog phone and check that the dial tone is heard when the phone goes off-hook. If the phone does not go off-hook, check that the port is not in a shutdown state. If the port is in a shutdown state, issue the **no shutdown** command.

Note Cisco IOS Software Release 12.2 and earlier provide dial tone, but Cisco IOS Software Release 12.3 and later require at least one dial peer to be defined on the router before an FXS will provide a dial tone.

- **Using Cisco CallManager, the FXO card does not send or pulse out digits.** The solution to this problem involves the following four-step procedure:

1. If the FXO connects to an FXS port on your PBX or PSTN, and the telephony devices are not receiving DTMF tones from the router FXO port, ensure that the **dial-peer voice pots** command is configured to forward digits.

By default, the router or gateway matches and strips exact destination patterns, as is shown in the following example:

```
!  
dial-peer voice 1 pots  
destination-pattern 123  
port 1/1/1  
!
```

2. If the router does not pulse out any digits on 123, be sure that the correct prefix or forward digits are configured for forwarding the desired digits as shown in the following example:

```
!  
dial-peer voice 1 pots  
destination-pattern 123  
  
forward-digits 3  
port 1/1/1  
!
```

Note For more information, refer to the “Digit Stripping on Outbound POTS Dial Peers” section of *Configuring Dial Plans, Dial Peers, and Digit Manipulation* at http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a0080080aec.html.

3. If you have the correct POTS peer configured, and you are still not receiving digits, make sure that the router is sending the correct DTMF tones by issuing the **debug vtsp dsp** command and making the call while capturing the logs. This log indicates each tone with a few lines of text, including “digit=1” and the exact frequencies of the tone. If you see the correct digits pulsed out, then the router is sending the digits.
 4. If the PBX or PSTN is not receiving digits, you need to check the values on the other end of the wire with a “T-berd” or analyzer. If you see duplicate or missing digits in the logs, this could indicate a problem with DSPs or incorrect digits received from the originating gateway. If the frequencies of the digits are not recognized, then the correct tones cannot be pulsed out. Make sure you issue the **dtmf-relay** command on the dial peers, especially if you have a very low bit rate codec configured.
- **The phone continues to ring on an FXO or FXS network after the user hangs up.** This problem occurs with only FXO loopstart signaling to PBX or PSTN devices (which do not have battery reversal or power denial) because the router FXO port is like a phone. The user must hang up the call so that it disconnects the line. In this case, there is an incorrect destination, sequence, number of rings, state, indication, result, or other outcome. The workaround for this problem is beyond the scope of this course. Please refer to *Cisco Systems Inc. Understanding FXO Disconnect Problems* at http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800ae2d1.shtml.

- **No dial tone is received from the gateway voice port after the phone goes off-hook.** If the Cisco IOS gateway is correctly configured, and there is no dial tone from the router when the phone or PBX goes off-hook, perform the following steps:
 1. Check to see if the voice ports are in administratively shutdown mode. In this mode, no dial tone is played. To check the dial tone, issue the **show voice port [slot-number]** command.
 2. To enable the ports, issue the **no shutdown** command under voice-port mode in the configuration.
 3. Make sure that the **direct-inward-dial** command is not configured under the **dial-peer voice pots** command. DID is not supported on analog FXO and FXS cards. DID is only supported on VIC-DID cards. If DID is configured on FXO and FXS cards, it can disable the dial tone and usually returns a fast busy signal. Remove this feature from the configuration and try again.
 4. Check to see if you have the private line, automatic ringdown (PLAR), or trunk configured under the voice port. If either of these conditions exists, the local dial tone will be disabled, too. To test for the local dial tone, temporarily remove the **connection plar** or the **connection trunk** commands. Reset the voice ports by issuing the **shutdown** and **no shutdown** commands, and check for the dial tone again.
 5. Check to see if the dial tone is being played but not heard by the remote phone. Issue the **debug voip ccapi inout** Cisco IOS software command, go off-hook, and look for a ccGenerateTone function in the output. If ccGenerateTone occurs in the output, the router is generating a tone. This symptom indicates that the transmit and receive pin-outs may be wired incorrectly.
 6. If you do not see any debugs, check to see that they are enabled to play on the console. Issue the terminal monitor command on the command line, and issue the **show debugging** Cisco IOS software command. Make sure that the debugs are enabled. Issue the **debug vpm all** command to monitor for voice-port telephony signaling. If you do not receive any debugs, this could be caused by mis-wiring on the transmit and receive pins. Verify the RJ-11 tip and ring wiring.
- **The second FXS port shuts down when a call is placed on the first port:** Port 0 on a VIC-2FXS is designed to accommodate a U.S.-style two-line phone, instead of the more common European-style one-line phone. In addition to using pins three and four, pins two and five are also monitored by the voice port. If you have a phone handset of unknown origin, it is possible that pins two and five are wired to allow last number recall or call forwarding. If this is the case, port 0 on the VIC assumes you have a two-line phone, and it shuts down port 1 automatically. To remedy this situation, perform the following steps:
 1. Be sure only two wires are used on your RJ-11 cable from the gateway to the phone.

2. Verify that the cores in the RJ-11 add up to two and that they are the middle two wires. For example, if you have a four-pin RJ-11, the middle two wires would be pins two and three. If you have a six-pin RJ-11, these wires would be pins three and four.

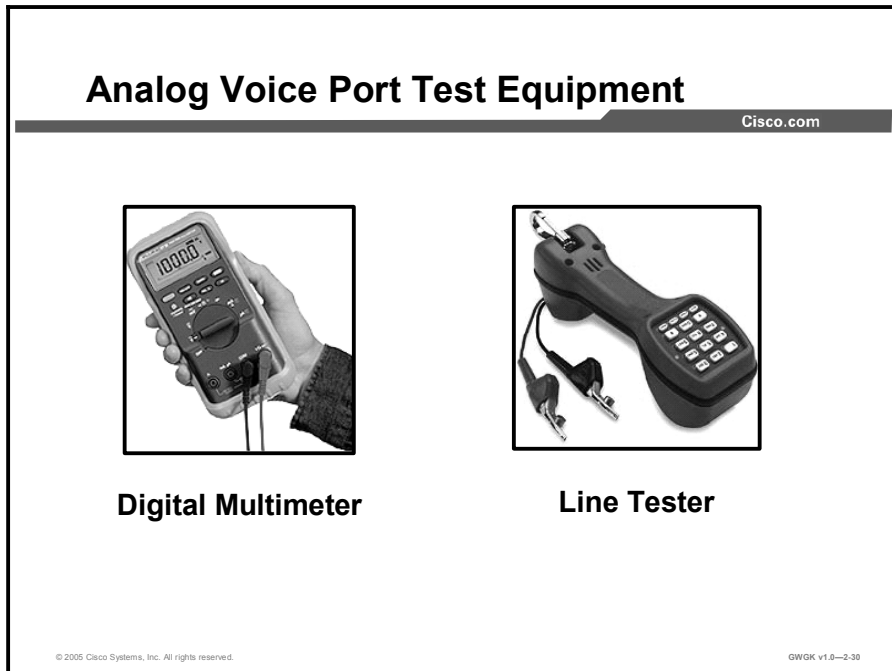
The following schematic shows port B with the following pin-out:

Pin 1 NC
Pin 2 port A tip
Pin 3 port B ring
Pin 4 port B tip
Pin 5 port A ring
Pin 6 NC

Note For more information, refer to “Common issues with the analog FXO and FXS circuits” at <http://www.ciscotacc.com/voice/showcase?case=K15416256>.

Troubleshooting Tools

This topic describes the troubleshooting tools that are used to resolve common analog issues.



The figure shows a typical technician line-test set: A digital multimeter and a line tester. While this equipment is not required for every installation, it is sometimes necessary to use test equipment to isolate problems with analog E&M ports. The most useful tools are a digital multimeter and a line tester. These tools allow the measurement of signaling states and voltages and allow the monitoring of audio signals.

The digital multimeter is used to measure the DC-loop voltage and AC-ringing voltage on FXS ports, E or M lead-signaling transitions, voltages on E or M leads, and the DC resistance of E&M signaling leads.

In the terminating mode of operation and when it is connected to a loopstart, the technician line tester acts like a normal telephone handset trunk and allows telephone numbers to be dialed on the inbuilt keypad. When switched to the monitoring mode (bridging mode), the unit presents a high impedance to the transmit (Tx) or receive (Rx) audio pairs of the E&M port. This impedance allows the audio signals and tones to be heard on the inbuilt loudspeaker. This feature helps find issues with one-way audio, incorrect digits that are sent or received, distortion and level problems, and possible sources of noise and echo. These are additional cabling tools:

- RJ-11 cables (straight-through, two conductors, and tip and ring are the preferred types)
- RJ-11 connector ends and spare two-conductor RJ-11 cable
- RJ-11 crimpers
- RJ-11 or RJ-45 cable extenders
- Oscilloscope (if available)
- Regular analog telephones

E&M Port-to-Port Testing

Cisco.com

The “rollover” cable has the following RJ45 connector wiring and can be used to connect two E&M ports for troubleshooting:

E&M Port 1	E&M Port 2
1	8
2	7
3	6
4	5
5	4
6	3
7	2
8	1

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-2.31

The experience of Cisco Technical Assistance Center (TAC) engineers has shown that the majority of faults with E&M ports are due to incorrect wiring or PBX port programming. To assist in determining if the fault is external to the router, it is possible to use the standard “rollover” cable. This rollover cable connects the signaling output of one port to the input of the other port and maintains an audio path between the two ports. To prove the operation of the router, dial peers can be configured to send a test call out one port, which is then looped back into the second port.

The figure shows the wiring for a rollover cable. The signaling crossover occurs as pins 2 (M lead) and 7 (E lead) on one port are connected to pins 7 (E lead) and 2 (M lead) on the other port. The two ports share a common internal ground. The crossover on pins 4 and 5 (audio pair) have no effect on the audio signal. By setting both voice ports to 2-wire, type-5 operation, the E&M ports become symmetrical and an outward seizure on one port is seen as an incoming seizure on the second port. Any DTMF digits sent out immediately come back and are then matched on another dial peer.

E&M Port-to-Port Testing (Cont.)

Cisco.com

```
voice-port 1/0/0
!--- First port under test.
operation 2-wire
signal-type wink
type 5
!
voice-port 1/0/1
!--- Second port under test.
operation 2-wire
signal-type wink
type 5
!
dial-peer voice 100 pots
!--- Send call out to port 1/0/0, strip the
!--- 100 and prefix with a called
!--- number 200.
destination-pattern 100
port 1/0/0
prefix 200
!
dial-peer voice 200 voip
!--- Incoming test call for 200 comes
!--- in on port 1/0/1 and is sent to 1.1.1.1 as VoIP call.
destination-pattern 200
session-target ipv4:1.1.1.1
!
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.32

When a VoIP call comes into the router with a called number of 100, it is sent out port 1/0/0. By default, any explicitly matched digits on a POTS dial peer are assumed to be an access code, and these codes are stripped off before the call is made. To route the call correctly, these digits must be replaced. In the example, the **prefix** command prepends the digits “200” as the called number. This call is immediately looped back in on port 1/0/1, the digits match on dial peer 200, and then the new call is made to the designated IP address. At this point, the devices originating and accepting the VoIP calls should then have an audio connection. This audio connection will span the IP network going out and coming in the E&M ports proving that the router is working properly. It also proves that the fault is not with the router.

Note In the configuration example in the figure, it is assumed that there are working devices on the IP network that can originate and accept VoIP calls.

Common VoIP Debug Commands

Cisco.com

Router#

```
debug voip ccapi [error|inout]
```

- Traces the execution path through the call control API

Router#

```
debug vpm all
```

- Enables all of the debug commands

Router#

```
show call active voice
```

- Displays the contents of the active call table

Router#

```
show call history voice
```

- Displays the contents of the call history table

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-2.34

The “VoIP Debug Commands” table lists and describes some of the common commands used to troubleshoot analog trunk connections.

VoIP Debug Commands

Command	Description
<code>debug voip ccapi [error inout]</code>	<p>This command is used to trace the execution path through the call control application program interface (API). The API serves as the interface between the call session application and the underlying network-specific software. You can use the output from this command to understand how calls are being handled by the router.</p> <p>The error keyword displays the errors in the call control API (CCAPI). This keyword shows error events or unexpected behavior in system software.</p> <p>The inout keyword displays the execution path through the CCAPI. The output from this command shows how calls are being handled by the router. This keyword shows how a call flows through the system, including call setup and teardown operations performed on both the telephony and network call legs.</p>
<code>debug vpm all</code>	<p>This command is used to enable all of the debug commands, such as the on-hook command and the off-hook command, for the voice port module and to view digits in the traffic flow.</p> <p>Caution: This debug will generate lots of output.</p> <p>It is usually a good idea to turn off all debugging and then enter the debug commands you are interested in one by one. This will help to avoid confusion about which ports you are actually debugging.</p> <p>Use one of the following voice port module (VPM) variants as required: debug vpm spi, debug vpm signal, and debug vpm dsp.</p>

Command	Description
<pre>show call active voice [brief [id identifier] compact [duration {less time more time}] echo- canceller call-id id identifier / redirect {rtpvt tbct}]</pre>	<p>Use this command to display the contents of the active call table.</p> <p>This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information for voice calls and fax relay calls that are currently connected through the router.</p> <p>There are many argument options to this command. The following describes some of the more useful arguments:</p> <ul style="list-style-type: none"> ■ brief: (Optional) Displays a truncated version of the contents. ■ duration: (Optional) Displays active calls that are longer or shorter than a specified <i>time</i>. The arguments and keywords are as follows: <ul style="list-style-type: none"> — less: Displays calls shorter than <i>time</i>. — more: Displays calls longer than <i>time</i>. — <i>time</i> : Elapsed time, in seconds. Range is from 1 to 2147483647. There is no default value. ■ echo-canceller call-id : (Optional) Displays information about the state of the extended echo canceller (EC). To query the echo state, you need to know the hex ID in advance. To find the hex ID, enter the show call active voice brief command or use the show voice call status command. The range is from 0 to FFFFFFFF.
<pre>show call history voice [brief [id identifier] compact [duration {less time more time}] [id identifier] last number redirect {rtpvt tbct}]</pre>	<p>Use this command to display the call history table. The call history table lists all calls connected through this router in descending time order since VoIP was enabled. You can display subsets of the call history table by using specific keywords.</p> <p>The arguments for the show call history voice command are similar in function and intent as the arguments for the show call active voice command.</p>

Common VoIP Debug Commands (Cont.)

Cisco.com

Router#

```
show voice port
```

- Displays configuration information about a specific voice port

Router#

```
debug voip rtp
```

- Enables debugging for RTP packets

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-2.35

The “VoIP Debug Commands (Cont.)” table describes additional common commands that are used to troubleshoot analog trunk connections.

VoIP Debug Commands (Cont.)

Command	Description
<code>show voice port</code>	Use this command to display configuration information about a specific voice port.
<code>debug voip rtp {error session [nse multicast conference dtmf-relay named-event] packet remote-ip ipaddress remote-port portnum packetnum packet callid idnum packetnum}</code>	<p>Use this command to enable debugging for Real-Time Transport Protocol (RTP) named event packets. To disable debugging output, use the no form of this command. A description of the required arguments follows:</p> <ul style="list-style-type: none"> ■ error: This argument prints out a trace for error cases. ■ session: This provides all session debug information. If used with a keyword, this will supply more specific debug information according to the keywords used. ■ named-event: (Optional) Provides debug information for Named Telephone Event (NTE) packets. <p>Caution: This command severely impacts performance and should be used only for single-call debug capture. Cisco does not recommend using this command when using fax relay because it can adversely affect fax relay.</p>

Note Certain **show** commands are supported by the Cisco Output Interpreter Tool, which allows you to view an analysis of **show** command output. The Cisco Output Interpreter is available at www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl.

Note Before issuing debug commands, please see *Important Information on Debug Commands* at http://www.cisco.com/en/US/tech/tk801/tk379/technologies_tech_note09186a008017874c.shtml.

```
Router# debug voip ccapi inout
!
cc_api_call_setup_ind (vdbPtr=0x60BFB530, callInfo={called=, calling=, fdest=0},
callID=0x60BFAEB8)
!
cc_process_call_setup_ind (event=0x60B68478) sess_appl: ev(14), cid(1), disp(0)
ccCallSetContext (callID=0x1, context=0x60A7B094) ccCallSetPeer (callID=0x1,
peer=0x60C0A868, voice_peer_tag=2, encapType=1, dest-pat=+14085231001, answer=)
!
ccCallSetupAck (callID=0x1)
!
cc_api_call_digit (vdbPtr=0x60BFB530, callID=0x1, digit=4, mode=0)
sess_appl: ev(8), cid(1), disp(0)
ssa: cid(1)st(0)oldst(0)cfid(-1)csize(0)in(1)fDest(0)
cc_api_call_digit(vdbPtr=0x60BFB530, callID=0x1, digit=1, mode=0)
sess_appl: ev(8), cid(1), disp(0)
ssa:cid(1)st(0)oldst(0)cfid(-1)csize(0)in(1)fDest(0)
!
```

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-2-36

The figure shows a screen capture of an output example from the **debug voip ccapi inout** command. The first highlighted output shows that the call setup has been accepted by the router. The second and last highlighted output show that the caller has entered DTMF digits twice before a dial peer is matched.

Showing Active Calls

Cisco.com

```
Router# show call active voice
Total call-legs:2
.
.
.
VOIP:
ConnectionId[0x7F8D82A4 0x928E11D5 0x8094FCFB 0x1C38F0FA]
IncomingConnectionId[0x7F8D82A4 0x928E11D5 0x8094FCFB 0x1C38F0FA]
RemoteIPAddress=172.29.248.111
RemoteUDPPort=17394
RoundTripDelay=4 ms
SelectedQoS=best-effort
tx DtmfRelay=inband-voice
FastConnect=TRUE
AnnexE=FALSE
.
.
.
LostPackets=0
EarlyPackets=0
LatePackets=0
.
.
.
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-3.37

The figure shows a screen capture of an output example from the **show call active voice** command. The first highlighted output shows the IP of the remote address. The second highlighted output indicates that the network is working well.

Showing Call History

Cisco.com

```
Router# show call history voice
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Total call-legs: 2
GENERIC:
SetupTime=85975291 ms
.
.
.
CallDuration=00:00:40
.
.
.
VOIP:
ConnectionId[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
.
.
.
GENERIC:
SetupTime=85975290 ms
.
.
.
TELE:
ConnectionId=[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-3.38

The figure shows a screen capture of an output example from the **show call history voice** command. The highlighted output shows the call set up times, how long the call took, the VoIP IP address, and the telephone IP address in hexadecimal.

Showing Voice Ports

Cisco.com

```
Router# show voice port 1/0/0
Foreign Exchange Station 1/0/0 Slot is 1, Sub-unit is 0, Port
is 0
Type of VoicePort is FXS
.
.
.
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Analog Info Follows:
Region Tone is set for northamerica
Currently processing none
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Voice card specific Info Follows:
Signal Type is loopStart
Ring Frequency is 25 Hz
Hook Status is On Hook
Ring Active Status is inactive
Ring Ground Status is inactive
Tip Ground Status is inactive
Digit Duration Timing is set to 100 ms
InterDigit Duration Timing is set to 100 ms
Hook Flash Duration Timing is set to 600 ms
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.39

The figure shows a screen capture of an output example from the **show voice port** command for an FXS analog voice port on a Cisco 3600 router. The first highlighted output shows that the voice port is configured as an FXS interface. The next two highlighted outputs show the start of the analog and voice card specific information.

Showing Voice RTP Session Information

Cisco.com

```
Router# debug voip rtp session named-event
00:09:29:      Pt:99   Evt:1   Pkt:03 00 00  <<<Rcv>
00:09:29:      Pt:99   Evt:1   Pkt:03 00 00  <<<Rcv>
00:09:29:      Pt:99   Evt:1   Pkt:03 00 00  <<<Rcv>
...
00:09:29:      Pt:99   Evt:1   Pkt:83 04 C8  <<<Rcv>
00:09:29:      Pt:99   Evt:1   Pkt:83 04 C8  <<<Rcv>
00:09:29:      Pt:99   Evt:1   Pkt:83 04 C8  <<<Rcv>
00:09:29:      Pt:99   Evt:2   Pkt:03 00 00  <<<Rcv>
...
00:09:29:      Pt:99   Evt:3   Pkt:03 00 00  <<<Rcv>
...
00:09:31: <Snd>>> Pt:99   Evt:9   Pkt:02 00 00
...
00:09:31: <Snd>>> Pt:99   Evt:8   Pkt:02 00 00
...
00:09:31: <Snd>>> Pt:99   Evt:7   Pkt:02 00 00
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-2.40

The figure shows a screen capture of debugging output for the **debug voip rtp session named-event** command. The example shows a gateway that sends digits 1, 2, 3, then receives digits 9, 8, and 7. The output that indicates the sent and received digits has been emphasized. The payload type, event ID, and additional packet payload are shown in each log.

The first highlighted output shows that the first three packets indicate the start of the tone (initial packet and two redundant). The last highlighted output shows the three packets that indicate the end of the tone (initial packet and two redundant). The packets in between are refresh packets that are sent every 50 ms (without redundancy).

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **FXO and E&M are common analog trunk connections to gateways.**
- **There are a number of common analog trunk features providing enabling phone features, caller id features, call waiting features, and call transfer features.**
- **To support E911, service providers typically require a CAMA interface on the client-side voice gateway.**
- **NMs and VICs are used in Cisco gateways to support analog trunks.**
- **The Cisco VG224, Cisco VG248, Cisco CMM, Cisco NM-HAD, and the Cisco EVM are used to provide high-density analog endpoints.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—2-41

Summary (Cont.)

Cisco.com

- **The router voice-ports must be configured to transmit and receive the same type of signaling that is used by the device sending the signaling.**
- **The most useful equipment to troubleshoot analog lines are the digital multimeter and the line test set.**
- **Common debug commands include debug voip, ccapi inout, debug vpm all, show call active voice, show call history voice, show voice port, and the debug vtsp all command.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—2-42

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) When an E911 call is placed, how is the calling number used by the PSAP? (Choose two.) (Source: Trunk Features)
- A) The PSAP uses the calling number to reference the ALI database to find the exact location of the caller.
 - B) The PSAP uses the called number to reference the ALI database to find the exact location of the caller.
 - C) The PSAP uses the calling number to reference the ANI database to find the exact location of the caller.
 - D) The PSAP uses the calling number as a callback number in case the call is disconnected
- Q2) What are VIC cards and how are they installed in Cisco routers? (Source: Router Analog Hardware Types)
- A) VICs are network modules that fit into HVIC interfaces in the Cisco ISR 3800 series router to provide the interface to telephony equipment and the PBX.
 - B) VICs are daughter cards that integrate with voice NM-HDAs to provide the interface to telephony equipment and the PSTN in the Cisco ISR 3800 series router.
 - C) VICs are daughter cards that integrate with voice NMs to provide the interface to telephony equipment and the PSTN in the Cisco 1700, 2800, and 3800 series routers.
 - D) VICs are network modules that provide the interface to telephony equipment and the PSTN the Cisco 1700, 2800, and 3800 series routers.
- Q3) Which Cisco analog voice gateway supports the Cisco CallManager Express with redial, call forward all, and speed dial? (Source: Router Analog Hardware Types)
- A) The VG248 Analog Phone Gateway (SCCP)
 - B) The VG224 Analog Phone Gateway (SCCP)
 - C) The VG200 with a VIC2-2FXS
 - D) The VG224 Analog Phone Gateway (MGCP)
- Q4) The client is complaining of echo and clipped or fuzzy voice quality on their Cisco IP phones. The client uses E&M signaling over an analog trunk to connect to the PSTN. What is the likely cause and why? (Source: Common Issues)
- A) Cabling problems because the majority of echo-based and voice-quality-based faults are with E&M ports that are incorrectly wired
 - B) FXO disconnect because supervisory disconnect has not been configured on the voice port so the PSTN has become overloaded, which results in echo and voice-quality problems
 - C) Impedance mismatch because the impedance has been set incorrectly so echo is generated and is affecting the voice quality
 - D) Voice volume because incorrect input or output levels can cause echo and too much input gain can cause clipped or fuzzy voice quality

Q5) Describe how to use a technician line tester to find possible sources of noise and echo.

Q6) The client had been experiencing voice quality problems related to dropped packets on the gateway. This problem has been fixed. Now the client is complaining of severe performance problems with the fax-relay services. What debug command has been left enabled, and why would it cause this problem? (Source: Troubleshooting Tools)

- A) The **debug voip rtp session named-event** command has been left enabled. This command severely affects fax-relay performance and should be used only for single-call debug capture.
- B) The **debug vpm all** command has been left enabled. This command generates a significant amount of output on packet information in the traffic flow, which, if left enabled, takes most of the processing cycles from all services including fax-relay services. This command should only run during periods of low VoIP traffic.
- C) The **debug voip ccapi inout** command has been left enabled. This command shows how calls are set up and torn down. This command generates output for both the telephony and network call leg. Consequently, it severely affects the performance of fax-relay services.

Lesson Self-Check Answer Key

Q1) A, D

Q2) C

Q3) B

Q4) D

Q5) The description should cover the following points: When switched to the monitoring mode, (bridging mode), the technician line tester presents a high impedance to the Tx or Rx audio pairs of the E&M port. This impedance allows the audio signals and tones to be heard on the inbuilt loudspeaker of the technician line tester. This feature helps find issues with one-way audio, incorrect digits that are sent or received, distortion and level problems, and possible sources of noise and echo.

Q6) A

Lesson 3

CAS Circuits

Overview

This lesson describes how to integrate a voice gateway to the public switched telephone network (PSTN) or a PBX using channel associated signaling (CAS) circuits. The lesson starts with a description of CAS and the types of CAS circuits that are used in North America. The lesson then presents a comparison of E1 R2 theory to North American CAS, presents common CAS issues network administrators deal with during gateway deployment, and describes how to configure a gateway to support CAS connections. The lesson finishes with a description of how to use troubleshooting tools to resolve common CAS issues.

Objectives

Upon completing this lesson, you will be able to integrate a voice gateway into the PSTN or a PBX using CAS circuits. This includes being able to meet these objectives:

- Describe CAS
- Describe the CAS types used in North America
- Describe E1 R2 signaling and compare it to North American CAS
- Configure a gateway to support CAS connections
- Describe the troubleshooting tools used to resolve CAS issues

Channel Associated Signaling

This topic describes CAS.

CAS

Cisco.com

- **CAS is a method of signaling each traffic channel rather than having a dedicated signaling channel.**
- **Signaling for a particular traffic circuit is permanently associated with that circuit.**
- **The most common forms of CAS signaling are:**
 - **Loop-start**
 - **Ground-start**
 - **E&M**
 - **There are several versions of E&M signaling.**
- **CAS processes the receipt of DNIS and ANI information.**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-2.3

CAS, also referred to as “robbed-bit signaling” in North America, is a method of signaling each traffic channel rather than using a dedicated signaling channel like ISDN. In other words, the signaling for a particular traffic circuit is permanently associated with that circuit. The most common forms of CAS are loop-start, ground-start, and receive and transmit (E&M). The biggest disadvantage of CAS is that it uses user bandwidth to perform signaling functions. In addition to receiving and placing calls, CAS also processes the receipt of dialed number identification service (DNIS) and automatic number identification (ANI) information. DNIS identifies the telephone number of the incoming call, and it is a common feature of 800 and 900 lines. ANI identifies the telephone number of the calling party. Service providers determine how this information is provided.

To implement CAS circuits, configure the physical layer (clocking, framing, and line-coding configurations), then match the configurations on each side of the CAS trunk. If one side is configured for wink-start and the other is configured for immediate-start, the call fails. It is important to have a good knowledge of the types of signaling used in order to identify the signaling requirements of the PBX or the PSTN.

T1 CAS Signaling

This topic describes the CAS signaling types that are used in North America.

Loop-Start Signaling

Cisco.com

- **Simplest form of CAS signaling**
- **Inability to notify upon a far-end disconnect or answer**
- **Loop-start uses the following to communicate call information:**
 - **FXS side only uses the A-bit**
 - **FXO side only uses the B-bit**
- **Susceptible to glare**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.8--2.4

Loop-start signaling is one of the simplest forms of CAS. However, a critical disadvantage of loop-start signaling is its inability to generate a notification indicating a far-end disconnect or answer. For instance, a call is placed from a Cisco router configured for Foreign Exchange Station (FXS) loop-start. Using loop-start signaling, when the remote end answers the call or when the remote end disconnects the call, there is no supervisory information sent to the Cisco router and, of course, the Cisco router can not relay information it does not have.

With loop-start signaling, the FXS side only uses the A-bit and the Foreign Exchange Office (FXO) side only uses the B-bit to communicate call information. A- and B-bits are bidirectional.

Note It is possible for answer supervision to be provided with loop-start connections if the network equipment can handle line-side answer supervision. Also, loop-start provides no incoming call channel seizure. Therefore, the network could experience glare (where both the FXO and FXS try to simultaneously place calls).

Ground-Start Signaling

Cisco.com

- **Similar to loop-start signaling**
- **Prevents glare by seizing the outgoing channel using the A-bit and B-bit on the network side instead of just the B-bit**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-3.5

Ground-start signaling is very similar to loop-start signaling. The clear advantage of ground-start signaling over loop-start signaling is the ability for incoming calls (from the network to the customer premises equipment [CPE]) to seize the outgoing channel. When the outgoing channel is seized, glare is prevented.

The outgoing channel is seized by using the A- and B- bit on the network side; loop-start signaling uses just the B-bit. On the CPE, the A-bit is used, but the B-bit involvement is dependent on the switch implementation. Typically, the B-bit is ignored by the service provider.

E&M Signaling

Cisco.com

- Is used for trunk lines
- Provides disconnect and answer supervision and glare avoidance
- Is simple to understand and is the preferred choice when implementing T1 CAS trunks
- Includes wink-start, immediate-start, and delay-start
 - The majority of T1 CAS circuits use E&M wink start signaling

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0—2.6

E&M signaling is typically used for trunk lines. E&M signaling has many advantages over the CAS methods. The key advantage of E&M signaling is that it provides disconnect and answer supervision in addition to glare avoidance. E&M signaling is simple to understand and is the preferred choice when using CAS. E&M has three types of signaling: wink-start, immediate-start, and delay-start. The majority of T1 CAS circuits use the E&M wink-start signaling type.

If there is a requirement to provide DNIS, then you must manually configure an appropriate signaling type. For example, E&M wink-start with DNIS support can be configured as E&M Feature Group-D (FGD).

Note Feature Group-B (FGB) also supports DNIS. FGB is configured using the E&M wink-start type on Cisco routers. DNIS is also supported on E&M immediate-signaling and delay-signaling types.

Feature Groups

Cisco.com

Feature Group	Description	Features
FGB	Used to notify the remote side that it can send the DNIS information	Outpulsing Alternate Traffic Routing ANI WATS Access Service Switched Transport Supervisory Signaling Line Termination Answer Supervision
FGD	A second wink that is sent to acknowledge the receipt of the DNIS information	Call supervision to an IEC Trunk-side access with an associated 10XXX access code Optional calling-party identification Recording of access-charge billing details Pre-subscription to a customer-specified IEC ANI for billing purposes
FGD - EANA	FGD-EANA provides emergency calls	Selective Routing Automatic Number Identification Automatic Location Identification

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-3.7

Telcordia Technologies, previously known as Bell Communications Research (Bellcore), developed several feature groups to support Direct Inward Dialing (DID) and other features on CAS circuits. The following describes the common feature groups that are used today:

- **FGB:** FGB or wink-start (also referred to a “FGA/B”) has unequal dialing parity. FGB notifies the called party that it can send DNIS information.
- **FGD:** FGD service is a trunk-side connection that enables telephone customers to choose their long distance network and use the same number of digits no matter which carrier they use. Cisco voice gateways interface with inter-exchange carriers (IXCs) using FGD to provide ANI in the carrier environment. None of the implemented CAS protocols, such as E&M-FGB, E&M immediate-start, FXS loop-start, FXS ground-start, single attachment station (SAS) loop-start, and SAS ground-start, provides support for such a service.

Note The other feature groups, A through C, are largely obsolete due to advances in telephony technology and legislation.

Cisco platforms use FGD to provide voice functionality in the carrier environment. FGD is a trunk-side local access transport area (LATA) access that supplies the following features:

- Call supervision to an IXC
- Trunk-side access with an associated 10XXX access code for end-user use in originating and terminating communications
- Optional calling-party identification
- Recording of access-charge billing details
- Presubscription to a customer-specified IXC
- ANI for billing purposes

FGD-exchange access North American (EANA) provides certain call services such as 911 emergency calls. The command **calling number outbound** is used only for FGD-EANA signaling to generate ANI digits for outgoing calls.

FGD-EANA implemented on a Cisco gateways can send and receive ANI; one digital signal level 0 (DS-0) group is configured to send ANI and the other DS-0 group is configured to receive ANI.

Note You must configure E&M-FGD to receive ANI and FGD-EANA to send ANI.

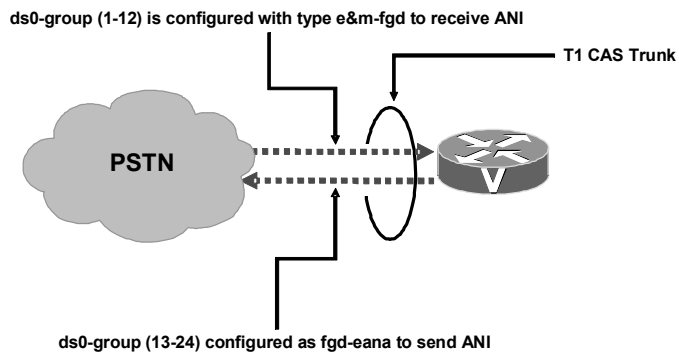
The following features are associated with FGD-EANA:

- **Selective Routing:** FGD-EANA electronically routes 911 emergency calls to the proper public safety answering point (PSAP) based on the emergency service number (ESN) code that has been assigned to the caller address.
- **ANI:** FGD-EANA provides the calling-party telephone number on a display at the PSAP.
- **Automatic Location Identification (ALI):** FGD-EANA stores the name and address associated with the calling-party telephone number on the display at the PSAP. The ANI looks up in the ALI database the name and address associated with the calling-party telephone number.

Note For supported digital H.323 and session initiation protocol (SIP) features for BRI, T1 CAS, T1 FGB, T1 FGD, and T1 Q Signaling (QSIG), see *Cisco IP Telephony Solution Reference Network Design (SRND) Cisco CallManager Release 4.0* page 130 of the PDF, downloadable at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a00802c370c.html.

T1 CAS Trunk Topology

Cisco.com



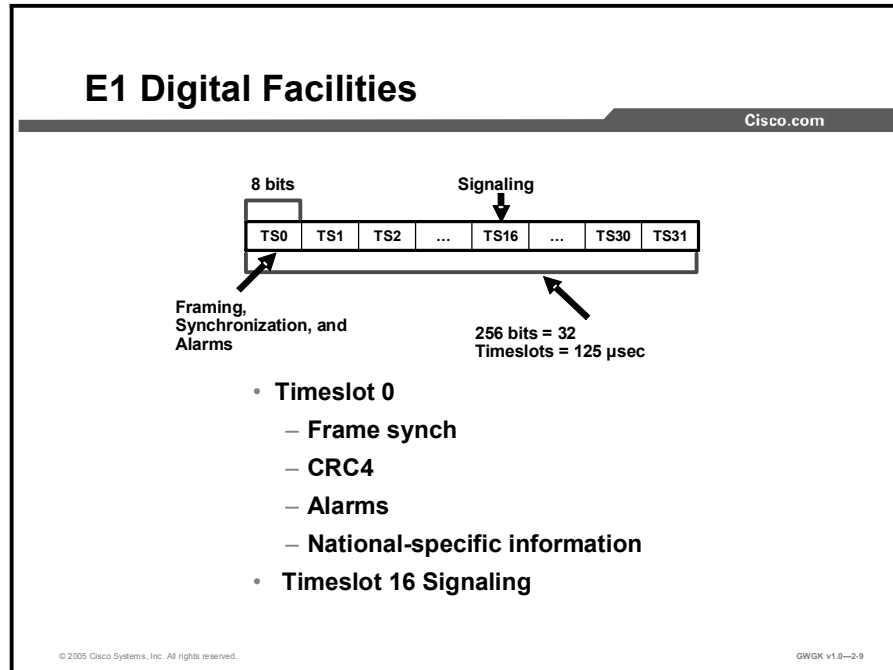
© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.8

If a location needs to send and receive ANI on a single T1, two DS-0 groups must be configured. One DS-0 group is configured with E&M-FGD to receive ANI and the second is configured as FGD-EANA to send ANI.

E1 R2

This topic describes E1 R2 signaling and compares it to North American CAS.



The E1 digital facilities carrier runs at 2.048 Mbps and has 32 timeslots. E1 timeslots are numbered TS0 to TS31. TS1 through TS15 and TS17 through TS31 are used to carry voice that is encoded with pulse code modulation (PCM) or to carry 64-kbps data. The figure shows the 32 timeslots of an E1 frame.

R2 Signaling

Cisco.com

- **R2 signaling operates across E1 digital facilities.**
- **Element types**
 - **Line signaling**
 - **R2 digital**
 - **R2 analog**
 - **R2 pulse**
 - **Supervisory signals**
 - **R2 interregister signaling**
 - **R2 compelled**
 - **R2 non-compelled**
 - **R2 semi-compelled**
 - **DTMF**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—2-10

R2 is channelized E1 signaling used in Europe, Asia, and South America. R2 is equivalent to channelized T1 signaling in North America. There are two types of R2 signaling: Line signaling and inter-register signaling.

Note The variations of R2 signaling for most countries are within the inter-register signaling configuration.

The three signaling types are described as follows:

- **Line signaling:** Line signaling includes the following types:
 - **R2 digital:** R2 line-signaling type ITU-U Q.421 is typically used for PCM systems (where A- and B-bits are used).
 - **R2 analog:** R2 line-signaling type ITU-U Q.411 is typically used for carrier systems (where a tone A-bit is used).
 - **R2 pulse:** R2 line-signaling type ITU-U Supplement 7 is typically used for systems that employ satellite links (where a tone A-bit is pulsed).

Note R2 pulse reflects the same states as analog signaling does, but the analog signal is a steady state (continuous signal), while the pulsed signal stays on for only a short time. “Pulsed” refers to a single pulse sent to reflect the state change.

- **Supervisory signals:** You can use line signaling, which uses TS16 (bits A, B, C, and D), for supervisory purposes such as handshaking between two offices for call setup and termination. In the case of ITU-T-R2 signaling, only bits A and B are used (bit C is set to 0 and bit D is set to 1). For two-way trunks, the supervision roles for forward and backward signaling vary on a call-by-call basis.

- **R2 inter-register signaling:** These signaling types are configured using the **cas-group (controller e1)** command. The following describes the four types of inter-register signaling:

- **R2 compelled:** When a tone pair is sent from the switch (forward signal), the tones stay on until the remote end responds (by sending an acknowledgment [ACK]). The remote responds with a pair of tones that signals the switch to turn off the tones. The tones are compelled to stay on until they are turned off.
- **R2 noncompelled:** The tone pairs are sent from the switch (forward signal) as pulses so that they stay on for a short time. Responses (backward signals) to the switch (Group B) are sent as pulses. There are no Group A signals in noncompelled inter-register signaling.

Note Most installations use the noncompelled type of inter-register signaling.

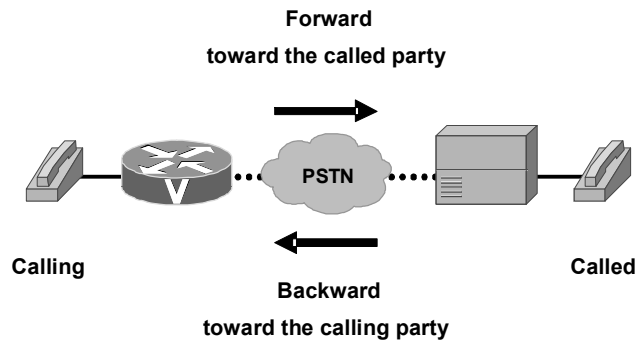
- **R2 semicompelled:** Forward tone pairs are sent as compelled signals. Responses (backward signals) to the switch are sent as pulses. R2 semicompelled signals are the same as compelled except that the backward signals are pulsed instead of continuous.
- **DTMF:** Inter-register signaling uses forward and backward in-band multifrequency signals in each timeslot to transfer called and calling party numbers, in addition to the calling party category. Some countries use two-out-of-six in-band DTMF signaling instead of forward and backward in-band multifrequency signals.

Note Do not use compelled signaling on slow (satellite) links. The call setup time would be too long because of distance delays.

Note Additional information on E1R2 can be found in *E1 R2 Signaling Theory* at http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800943c2.shtml.

R2 Interregister Signaling

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.11

The concept of address signaling in R2 is slightly different from that used in other CAS systems. In R2 signaling, the exchanges are considered registers and the signaling between these exchanges is called inter-register signaling. Inter-register signaling uses forward and backward in-band multifrequency signals in each timeslot to transfer called and calling party numbers, in addition to the calling party category. The figure clarifies illustrates forward and backward multifrequency signals and how these signals relate to the calling and called parties.

There are 15 forward signals that are classified into Group I and Group II forward signals. There are also 15 backward signals that are classified into Group A and Group B backward signals.

In most cases, Group I forward signals and Group A backward signals control call setup and transfer address information between the outgoing register (CO) and the incoming register (CPE). The incoming register can signal the outgoing register to change over to Group II and Group B signaling.

Group II forward signals provide the calling party category. Group B backward signals show the condition of the called subscriber line. Group B signals, also called "B tones", are typically the last tone in the protocol. For example, a B-3 tone indicates that the called party line is busy.

Signaling always begins with a Group I forward signal followed by a Group A backward signal that acknowledges the signal just received. This Group A backward signal may request additional information. Each signal requires a response from the other party. Each response becomes an acknowledgment of the event and an event to which the other party must respond.

Backward signals serve to indicate certain conditions encountered during call setup or to announce a switchover to changed signaling (for example, when forward signaling switches over to backward signaling). Changing to Group II and Group B signaling allows information about the state of the called subscriber line to be transferred.

The following identifies the forward and backward signal information:

■ **Group I signals (forward):**

- Represent the called party number or dialed digits.
- DNIS and ANI digits.
- I-1 to I-10 indicate digits 1 to 10.
- I-15 is the end of identification.

■ **Group II signals (forward):**

- Represent the calling party category.
- II-1 is indicates “subscriber without priority”.
- II-2 to II-9 indicate “subscriber with priority”.
- II-11 to II-15 are spare for national use.

■ **Group A signals (backward):** These signals indicate whether the signaling has ended or if a particular forward signal is required. Group A signals to acknowledge and convey signaling information.

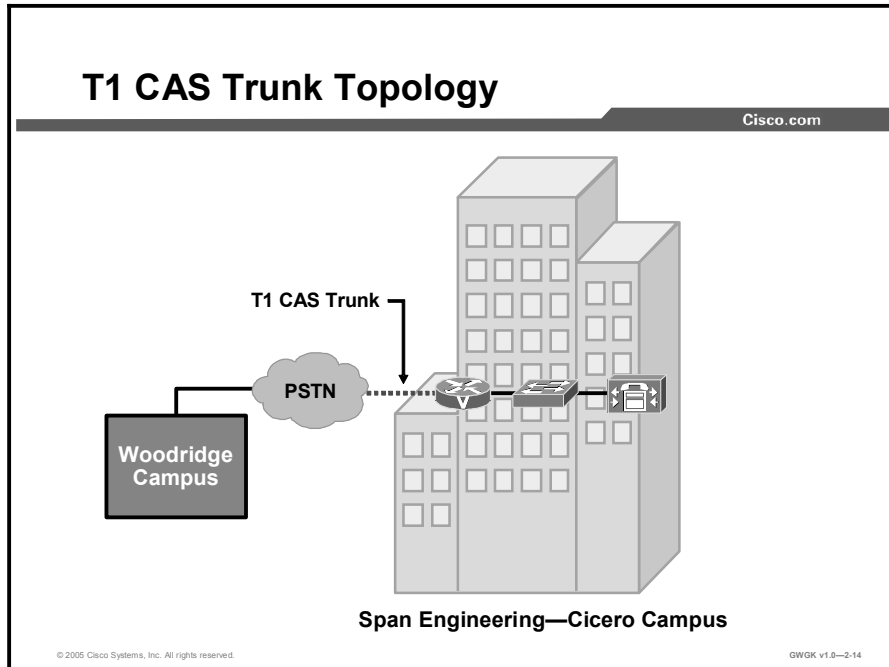
- A-1 indicates “send next digit”.
- A-3 indicates “address-complete” and “changeover to reception of Group B signals”.
- A-4 indicates congestion.
- A-5 indicates “send calling party category”.
- A-6 indicates “address complete”, “charge”, “setup”, and “speech conditions”.

■ **Group B signals (backward):** These signals are sent by the terminating switch to acknowledge a forward signal or to provide call charging and called party information. Group B signals are used to acknowledge Group II forward signals.

- B-3 indicates “subscriber line busy”.
- B-4 indicates congestion.
- B-5 indicates “unallocated number”.
- B-6 indicates “subscriber line free charge”.

CAS Configuration

This topic describes how to configure a gateway to support CAS connections. The description includes T1 and E1 R2 CAS connections.



The figure shows a sample T1 CAS topology. The dotted line between the PSTN and the voice gateway represents a T1 CAS trunk. The design calls for 12 channels providing ANI information for outgoing calls and 12 channels accepting ANI information for incoming calls.

Configuring T1 CAS

Cisco.com

Step	Action
1	Set up the T1 controller connected to the PSTN.
2	Define the line signaling use the following commands: <code>(config)#controller T1 0</code> <code>(config-controller)#ds0-group 1 timeslots 1-24 type ?</code>

Note: The “?” in the ds0-group command will provide different line-signaling options for the Cisco AS5xxx platforms and for the Cisco 2600/3600/3700 platforms.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—2-15

The “Configure T1 CAS” table provides the steps to configure T1 CAS.

Configure T1 CAS

Step	Action	Notes
1.	Set up the T1 controller connected to the PSTN.	Use the following options to ensure that the framing and line coding of the T1 are properly set: <ul style="list-style-type: none">■ T1 framing: Extended Superframe (ESF) or Superframe (SF)■ T1 line coding: Binary 8-zero substitution (B8ZS) or alternate mark inversion (AMI)■ T1 clock source: Internal or line Keep in mind that different PBXs have different requirements for the clock source.

Step	Action	Notes
2.	To define the line signaling, use the following commands: <pre>(config)#controller T1 0 (config-controller)#ds0-group 1 timeslots 1-24 type ?</pre>	The "?" in the ds0-group command provides different line-signaling options for the Cisco AS5000 Series gateways and for the Cisco 2600 Series, 3600 Series, and 3700 Series routers. Notes for the Cisco AS5000 Series platforms: <ul style="list-style-type: none"> ■ If you want to collect DNIS information on a T1 controller, you must manually configure it on the access server. ■ To collect DTMF DNIS for E&M-FGB under a controller T1 configuration, use the ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis command. ■ To collect multifrequency (MF) DNIS for E&M-FGB, use the ds0-group 0 timeslots 1-24 type e&m-fgb mf dnis command.

The following line-signaling types are available for the Cisco AS5000 Series gateways:

- **e&m-fgb**: E&M Type II FGB
- **e&m-fgd**: E&M Type II FGD
- **e&m-immediate-start**: E&M immediate-start
- **fgd-eana**: FGD-EANA
- **fgd-os**: FGD operator services
- **fxs-ground-start**: FXS ground start
- **fxs-loop-start**: FXS loop start
- **none**: Null signaling for external call control
- **r1-itu**: R1 ITU
- **sas-ground-start**: SAS ground start
- **sas-loop-start**: SAS loop start

The following line signaling types are available for the Cisco 2600 Series, 3600 Series, and 3700 Series routers:

- **e&m-delay-dial**: E&M delay dial
- **e&m-fgd**: E&M Type II FGD
- **e&m-immediate-start**: E&M immediate-start
- **e&m lmr**: E&M Land Mobile Radio (LMR)
- **e&m-wink-start**: E&M wink-start
- **ext-sig**: External signaling
- **fgd-eana**: FGD-EANA Bell operating company (BOC) side
- **fxo-ground-start**: FXO ground start
- **fxo-loop-start**: FXO loop start
- **fxs-ground-start**: FXS ground start
- **fxs-loop-start**: FXS loop start

Example: T1 CAS Configuration

Cisco.com

```
controller T1 2/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-12 type fgd-eana
 ds0-group 2 timeslots 12-24 type e&m-fgd

dial-peer voice 1 pots
 destination-pattern 9T
 port 2/0:1
!
dial-peer voice 9 pots
 incoming called-number .
 direct-inward-dial
 port 2/0:2
```

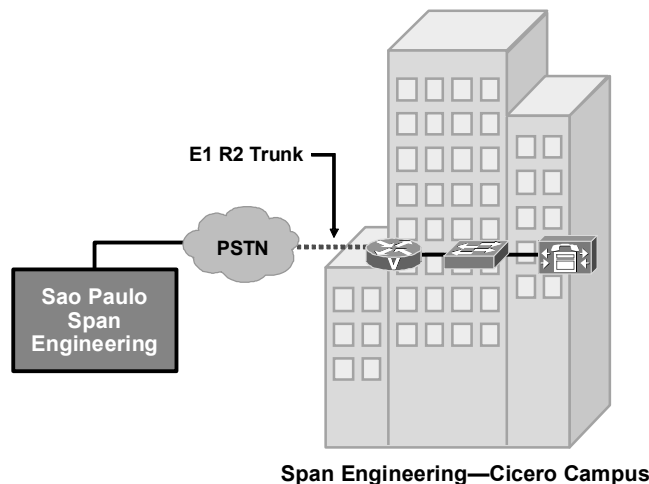
© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-16

The slide shows a screen capture of a T1 CAS sample configuration. The commands that enable T1 CAS are in the first highlighted line. The commands that split ANI receiving and sending onto separate DS-0 groups are in the second highlighted line. Notice that E&M FGD and E&M FGD-EANA are used.

E1 R2 Trunk Topology

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-17

The figure depicts a sample E1 R2 topology. The dotted line between the PSTN and the voice gateway represents an E1 R2 trunk. The design calls for an E1 trunk provisioned for ITU Q.421 digital line signaling and compelled register signaling to the Span Engineering South American subsidiary.

Configuring E1 R2

Cisco.com

- **Step 1: Enter global configuration mode.**

```
Router# configure terminal
```

- **Step 2: Specify the E1 controller to configure with R2 signaling.**

```
Router(config)# controller E1 1/0
```

- **Step 3: Configure R2 CAS on the E1 controller.**

```
Router(config-controller)# ds0-group 1 timeslots 1-31 type  
r2-digital r2-compelled ani
```

- **Step 4: Enter CAS custom mode and localize E1 R2 signaling parameters.**

```
Router(config-controller)# cas-custom 1  
Router(config-ctrl-cas)# country brazil use-defaults
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-18

The commands shown in the figure are some of the commands used to configure R2 signaling and customize R2 parameters on controller E1 1/0 of a Cisco 3640 Series router. In most cases, the same R2 signaling type is configured on each E1 controller. To configure support for E1 R2 signaling, use the commands presented in the “Configuring E1 R2” table, beginning in global configuration mode.

Configuring E1 R2

Step	Action	Notes
1.	<code>configure terminal</code>	Use this command to enter global configuration mode.
2.	<code>controller E1 slot/port</code>	<p>Use this command to specify the E1 controller that you want to configure with R2 signaling.</p> <p>A controller informs the router how to distribute or provision individual timeslots for a connected channelized E1 line. You must configure one E1 controller for each E1 line.</p> <p>There are slight differences in the commands used by different Cisco routers to configure E1 R2. For example, the controller e1 slot/port-adapter/port command is used by Cisco 7500 Series and Cisco 7000 Series routers with the RSP7000 and RSP7000CI.</p> <p>Please refer to the command reference of your router for the specific commands to use.</p>

Step	Action	Notes
3.	<code>ds0-group channel timeslots range type signal</code>	<p>Use this command to configure CAS.</p> <p>The R2 part of this command is defined by the <i>signal</i> variable in the ds0-group command.</p> <p>Replace the <i>signal</i> variable with any of the following choices under R2 analog, R2 digital, or R2 pulse:</p> <ul style="list-style-type: none"> ■ <i>r2-digital</i> dtmf ■ <i>r2-compelled</i> ani ■ <i>r2-non-compelled</i> ani ■ <i>r2-semi-compelled</i> ani
4.	<code>cas-custom channel</code>	<p>Enter CAS custom mode</p> <p>For the customizing to take effect, the <i>channel</i> number used in the cas-custom command must match the channel number specified by the cas-group command.</p>
	<code>country name</code>	<p>Use the <i>use-defaults</i> option to localize E1R2 signaling parameters as required:</p> <ul style="list-style-type: none"> ■ Replace the <i>name</i> variable with one of the supported country names. ■ It is recommended that you include the <i>use-defaults</i> option, which enables the default settings for a specific country. The default country setting is ITU.
Note	<p>For the list of supported countries, regions, and corporation specifications see the cas-custom command in the <i>Cisco IOS Dial Technologies Command Reference, Release 12.3 T</i> at http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_book09186a00801a7e84.html.</p>	

Example: E1 R2 Configuration

Cisco.com

```
!
configure terminal
controller e1 1/0
Router(config-controller)# cas-group 1 timeslots 1-31 type r2-digital
r2-compelled ani
cas custom 1
country brazil use-defaults
...
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-19

The figure shows a screen capture of an E1 R2 sample configuration. The commands that enable R2 digital, R2 compelled, and ANI are highlighted. The Brazil country code has been used as well as the recommended **use-defaults** command.

Troubleshooting CAS Circuits

This topic describes the troubleshooting tools you can use to resolve CAS issues.

Common CAS Issues

Cisco.com

- **Lack of physical layer connectivity**
- **Clocking information is obtained differently**
- **Signaling type is different on each router**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-2.20

The following lists the common CAS issues and the commands used to confirm them:

- **Trouble with physical layer connectivity:** To check the physical layer connectivity, use the **show controllers** command. This command shows the physical layer connectivity and the framing, line code, and clock source settings. Recall that the framing, line code, and clock source settings must match those for the switch to which the voice-enabled gateway is connected.
- **Clocking information is different on each router:** You must make sure that one side of the connection is providing the clocking and the other side of the connection is getting the clocking from the line.
- **Different signaling is being used on each router:** The T1 CAS must be the same on both ends of the trunk. One of the most common problems of T1 CAS is mismatched signaling. Using commands such as the **show voice summary** command provides a summary on the status of all the channels. Using debug commands such as the **debug vpm signal** provides the information for most T1 CAS problems.

CAS Troubleshooting Commands

Cisco.com

router#

```
debug serial interface
```

- Displays information on a serial connection failure

router#

```
show controller e1
```

- Displays the controller status specific to an E1 controller

router#

```
debug vtsp all
```

- Enables the digits exchanged between the PBX, PSTN, and the router

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-21

The figure provides some common CAS troubleshooting commands. The “CAS Troubleshooting Commands” table provides a detailed description of these commands.

CAS Troubleshooting Commands

Command	Description
<code>debug serial interface</code>	<p>To display information on a serial connection failure, use the debug serial interface command in privileged EXEC mode. To disable debugging output, use the no form of this command.</p> <p>If the show interface serial EXEC command shows that the line and protocol are down, you can use the debug serial interface command to isolate a timing problem as the cause of a connection failure. If the <code>keepalive</code>, <code>yourseen</code>, and <code>myseen</code> fields are not incrementing in each subsequent line of output, there is a timing or line problem at one end of the connection.</p>
<code>show controllers t1/e1 controller-number timeslots timeslot-range</code>	<p>This command shows whether the DS-0 channels of a controller are in idle, in-service, maintenance, or busyout states. Enter the show controllers t1/e1 command to display statistics about the T1 or E1 links.</p> <p>The following describes the syntax options:</p> <ul style="list-style-type: none"> ■ t1/e1: This variable indicates the interface type. ■ controller-number: This is the controller number of the CAS or ISDN PRI timeslot. The range is from 0 to 7. ■ timeslots: This variable displays DS0 information. ■ timeslot-range: The timeslot E1 range is from 1 to 31. The timeslot T1 range is from 1 to 24.

Command	Description
<pre>debug vtsp all</pre>	<p>This command enables the following debug vtsp commands:</p> <ul style="list-style-type: none"> ■ debug vtsp session ■ debug vtsp error ■ debug vtsp dsp. <p>For more information or for sample output, see the individual commands.</p> <p>Execution of the no debug vtsp all command turns off all Voice Telephony Service Provider (VTSP)-level debugging. You should turn off all debugging and then enter the debug commands you are interested in one by one. This process helps avoid confusion about which ports you are actually debugging.</p> <p>Caution: Using this command can severely impact network performance and prevent any faxes from succeeding.</p>

CAS Troubleshooting Commands (Cont.)

Cisco.com

```
router#  
debug vpm signal
```

- Debug line signaling on Cisco router platforms

```
router#  
debug cas
```

- Debug line signaling on Cisco AS5xxx platforms

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—2.22

CAS Debug Commands (Cont.)

Command	Description
<code>debug vpm signal</code>	This command collects debug information only for signaling events. This command can also be useful in resolving problems with signaling to a PBX.
<code>debug cas</code>	Use this command for line signaling on Cisco AS5000 gateways.

Note Before issuing debug commands, please see *Important Information on Debug Commands* at http://www.cisco.com/en/US/tech/tk801/tk379/technologies_tech_note09186a008017874c.shtml.

Showing E1 Controller State

Cisco.com

```
Router# show controllers e1
e1 0/0 is up.
  Applique type is Channelized E1 - unbalanced
  Framing is CRC4, Line Code is HDB3
  No alarms detected.
  Data in current interval (725 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs

  Total Data (last 24 hours)
    0 Line Code Violations, 0 Path Code Violations,
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.23

The figure shows a screen capture of an output example from the **show controllers e1** command on a Cisco 7500 Series router.

Revealing CAS E&M FGB Signaling

Cisco.com

```
Router#show debug
CAS:
  Channel Associated Signaling debugging is on
Router#
!--- Incoming call to router.
*May 28 12:40:35.376: from Trunk(0): (1/0): Rx LOOP_CLOSURE (ABCD=1111)
!--- Switch is off hook.
!--- Send wink back to the switch. Note we transition from a on/off/on hook state.
*May 28 12:40:35.600: from Trunk(0): (1/0): Tx LOOP_CLOSURE (ABCD=1111)
!--- Sending Wink back. Off hook.
*May 28 12:40:35.800: from Trunk(0): (1/0): Tx LOOP_OPEN (ABCD=0000)
!--- End of wink ~200 ms duration. On hook.
Router#
Router#
!--- The call is now in an alerting state waiting for a connect.
!--- Router goes off hook. Call is connected.
*May 28 12:40:37.352: from Trunk(0): (1/0): Tx LOOP_CLOSURE (ABCD=1111)
!--- Router has gone off hook. Send a connect.
Router#
Router#
Router#
!--- At this point, the call is torn down in the direction of the PBX.
*May 28 12:40:42.608: from Trunk(0): (1/0): Tx LOOP_OPEN (ABCD=0000)
!--- Router disconnects call on hook.
*May 28 12:40:42.940: from Trunk(0): (1/0): Rx LOOP_OPEN (ABCD=0000)
!--- Switch terminates upon receipt on hook.
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.24

The figure shows a screen capture of the information revealed by the **show debug CAS** command on a Cisco AS5300 gateway running E&M FGB signaling. The screen capture is annotated to describe what is happening at each step in the debug output.

Using debug vpm signal to Reveal Signaling Events

Cisco.com

- Shows that a ring is detected and that the router waits for the ringing to stop before accepting the call

```
ssm_process_event: [1/0/1, 0.2, 15] fxols_onhook_ringing
ssm_process_event: [1/0/1, 0.7, 19] fxols_ringing_not
ssm_process_event: [1/0/1, 0.3, 6]
ssm_process_event: [1/0/1, 0.3, 19] fxols_offhook_clear
```

- Shows the call is connected

```
ssm_process_event: [1/0/1, 0.3, 4] fxols_offhook_proc
ssm_process_event: [1/0/1, 0.3, 8] fxols_proc_voice
ssm_process_event: [1/0/1, 0.3, 5] fxols_offhook_connect
```

- Confirms a disconnect from the switch and release with higher layer code

```
ssm_process_event: [1/0/1, 0.4, 27] fxols_offhook_disc
ssm_process_event: [1/0/1, 0.4, 33] fxols_disc_confirm
ssm_process_event: [1/0/1, 0.4, 3] fxols_offhook_release
```

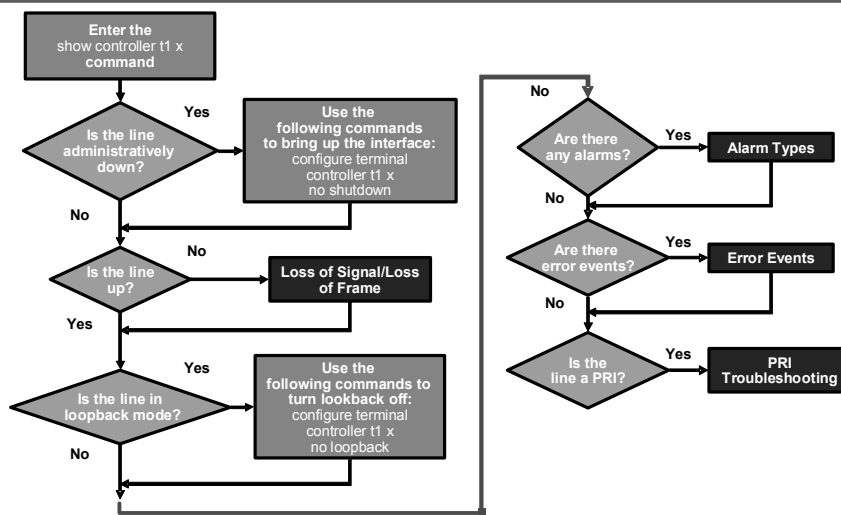
© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-25

The figure shows example output depicting typical signaling states that have been revealed using the **debug vpm signal** command.

T1 Troubleshooting Procedure

Cisco.com



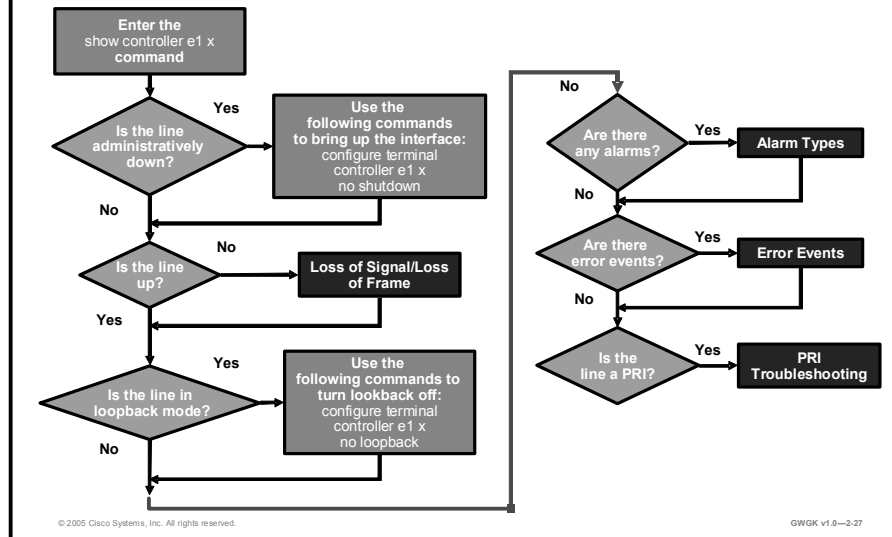
© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-26

The figure presents the T1 troubleshooting procedure. Cisco makes this table available as an interactive tool. To view and interact with this table see *T1 Troubleshooting* at http://www.cisco.com/en/US/tech/tk713/tk628/technologies_tech_note09186a00800a5f40.shtml.

E1 Troubleshooting Procedure

Cisco.com



The figure presents the E1 troubleshooting procedure. Cisco makes this table available as an interactive tool. To view and interact with this table *Troubleshooting* at http://www.cisco.com/en/US/tech/tk713/tk628/technologies_tech_note09186a00800a70fb.shtml.

Note For a comprehensive discussion on troubleshooting T1 and E1 CAS circuits see *Troubleshooting Digital Voice Interfaces to the IP Network* available at http://cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax_c/voipt_c/vtstele/vts_dgtl.htm#wp1002608.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

Cisco.com

- **CAS is a method of signaling each traffic channel. The signaling for a particular traffic circuit is permanently associated with that circuit.**
- **On T1 CAS DS-0 groups, you always need to configure E&M-FGD to receive ANI and FGD-EANA to send ANI.**
- **R2 signaling operates across E1 digital facilities.**
- **There are two elements to R2 signaling: Line signaling, which supports supervisory signals, and interregister signaling, which supports call setup control signals.**
- **Cisco.com has web-based interactive T1 and E1 troubleshooting tools.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—2-28

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) How is T1 CAS for a traffic circuit accomplished? (Source: T1 CAS)
- A) T1 CAS for a traffic circuit is permanently associated with that circuit.
 - B) T1 CAS for a traffic circuit has a dedicated signaling channel
 - C) T1 CAS uses out-of-band channels to associate signals with circuits.
- Q2) Describe the advantages to using E&M signaling over loop-start and ground-start signaling T1 CAS trunks. (Source: T1 CAS)
- _____
- _____
- _____
- _____
- _____
- Q3) If a client wanted call supervision, calling party identification, a record of access-charge billing, trunk-side access for end users, and ANI for billing details only, which feature group would the client choose? (Source: T1 CAS)
- A) FGD-EANA
 - B) FGB
 - C) FGD
 - D) FGA
- Q4) If a European client wished to use a satellite link to carry R2 line signaling, which type of R2 line signaling would the client use? (Source: E1 R2)
- A) R2-digital
 - B) R2-pulse-core
 - C) R2-pulse
 - D) R2-analog
- Q5) Which E1 timeslot and which bits can be used to send supervisory signals for call setup and termination handshaking between two offices? (Source: E1 R2)
- A) E1 timeslot 16 using only bits A and B with bit C set to 0 and bit D set to 1
 - B) E1 timeslot 16 using bits A, B, C, and D
 - C) E1 timeslot 0 using bits A, B, C, and D
 - D) E1 timeslot 15 using only bits A and B with bit C set to 0 and bit D set to 1

- Q6) After you configure R2 CAS on the E1 controller, what is the next step in the E1 configuration procedure? (Source: CAS Configuration)
- A) Define the line signaling for the DS-0 groups.
 - B) Specify the E1 controller you want to configure for R2 signaling.
 - C) Enter CAS custom mode and localize E1 R2 signaling parameters as required.
 - D) Specify the local country, region, or corporation specification to use with R2 signaling.
- Q7) A client thinks the framing, line code, and clock source settings do not match the switch that the voice-enabled gateway is connected to. Which troubleshooting command is used to check the physical layer connectivity of the T1 CAS trunk? (Source: Troubleshooting CAS Circuits)
- A) **show voice ports**
 - B) **show controllers**
 - C) **debug vpm signal**
 - D) **debug serial interface**
- Q8) After issuing the **debug vpm signal** command, the following debug output was observed:
- ```
ssm_process_event: [1/0/1, 0.2, 15] fxols_onhook_ringing
ssm_process_event: [1/0/1, 0.7, 19] fxols_ringing_not
ssm_process_event: [1/0/1, 0.3, 6]
ssm_process_event: [1/0/1, 0.3, 19] fxols_offhook_clear
```
- What does the last line show?
- A) The last line shows the router accepting the call.
  - B) The last line shows the router rejecting the call.
  - C) The last line shows the router clearing the call.

## Lesson Self-Check Answer Key

- Q1) A
- Q2) The description should cover the following points: E&M signaling is typically used for trunk lines. It has many advantages over the CAS methods previously discussed. E&M provides both disconnect and answer supervision as well as glare avoidance. E&M signaling is simple to understand and is the preferred choice when using CAS. E&M signaling includes wink start, immediate start, and delay start. The majority of T1 CAS circuits use E&M wink-start signaling.
- Q3) C
- Q4) C
- Q5) B
- Q6) C
- Q7) B
- Q8) A





## Lesson 4

---

# ISDN PRI Circuits

---

## Overview

ISDN circuits provide advantages over channel associated signaling (CAS) or “robbed-bit” circuits. For instance, the full 64-kbps bearer streams that are available in ISDN are perfectly compatible with the G.711 codec that is used in LANs for IP telephony. Consequently, as organizations migrate to IP telephony, they use ISDN BRI and PRI circuits to connect their voice gateways to PBXs and the public switched telephone network (PSTN).

The capabilities offered by ISDN make it complex. Depending on the manufacturer, the array of information that is passed in Q.931 messages is sometimes used slightly differently from switch to switch. If an organization is migrating to IP telephony, the different ways vendors can implement ISDN in PBX or PSTN switches can create problems where there logically should be none. This lesson describes how to setup a voice gateway with the two ISDN trunk variants.

## Objectives

Upon completing this lesson, you will be able to integrate a voice gateway into the PSTN or a PBX using PRI circuits. This includes being able to meet these objectives:

- Describe ISDN technology as it applies to deploying voice services
- Describe the ISDN signaling switch types used on the network and user sides
- Describe how ISDN passes messages on the D channel
- Describe IEs in ISDN signaling and how these elements are used by endpoints
- Describe how to select and configure the correct ISDN numbering plan
- Describe common ISDN issues that occur during gateway deployment
- Describe how to configure a gateway to support ISDN connections
- Describe the troubleshooting tools used to resolve ISDN issues

# ISDN Circuit Review

This topic describes ISDN technology as it applies to deploying voice services.

## ISDN Circuit Overview

Cisco.com

|                        | BRI                | T1 PRI              | E1 PRI              |
|------------------------|--------------------|---------------------|---------------------|
| <b>B-Channels</b>      | <b>2 x 64 kbps</b> | <b>23 x 64 kbps</b> | <b>30 x 64 kbps</b> |
| <b>D-Channels</b>      | <b>1 x 16 kbps</b> | <b>1 x 64 kbps</b>  | <b>1 x 64 kbps</b>  |
| <b>Framing</b>         | <b>16 kbps</b>     | <b>8 kbps</b>       | <b>64 kbps</b>      |
| <b>Total Data Rate</b> | <b>160 kbps</b>    | <b>1.544 Mbps</b>   | <b>2.048 Mbps</b>   |
| <b>Line Coding</b>     | <b>2B1Q / 4B3T</b> | <b>AMI / B8ZS</b>   | <b>HDB3</b>         |

**ISDN streams contain:**

- **Voice, video and data sent over separate B-channels**
- **Signaling data sent over a single D-channel used by all B-channels**

**Known as Common Channel Signaling (CCS)**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0 2-3

With ISDN, user data is separated from signaling data. User data, such as the payload from a digitized phone call, goes to a 64-kbps bearer channel (B channel) and signaling data, such as a call SETUP message, goes to a data channel (D channel). A single D channel supports multiple B channels, which is why ISDN service is known as common channel signaling (CCS).

ISDN traffic is carried on two types of trunks: The BRI and the PRI. BRI provides two B channels and a 16-kbps D channel, while PRI supports 23 (for T1) or 30 (for E1) B channels and a 64-kbps D channel. Either of these can connect the PSTN or a PBX to a Cisco voice gateway.

---

**Note** A single D channel can carry the signaling traffic for multiple PRIs using Non-Facility Associated Signaling (NFAS).

---

The benefits of using ISDN for voice traffic are as follows:

- ISDN is perfect for G.711 pulse code modulation (PCM) because each B channel is a full 64 kbps with no robbed bits.
- ISDN has a built-in call control protocol known as ITU-T Q.931.
- ISDN can convey standards-based voice features, such as speed dialing, automated operator services, call waiting, call forwarding, and geographic analysis of customer databases.
- ISDN supports standards-based enhanced dialup capabilities, such as Group 4 fax and audio channels.

---

**Note** ISDN BRI voice is commonly used in Europe. ISDN PRI voice is used worldwide.

---

## Non-Facility Associated Signaling (NFAS)

Cisco.com

- **Allows a single D channel to control multiple PRI interfaces**
- **A backup D channel can be configured, but only the NFAS primary D channel must be configured**
- **NFAS is only supported with a channelized T1 controller**
- **The router must connect to either a 4ess, dms250, dms100, or a National ISDN switch type**

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0 2-4

ISDN NFAS allows a single D channel to control multiple PRI interfaces, which allows one B channel on each interface to carry other traffic. A backup D channel can be configured for use when the primary NFAS D channel fails. However, once the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all the members of the associated NFAS group. When a backup D channel is configured, any hard failure causes a switchover to the backup D channel and connected calls remain connected.

NFAS is only supported with a channelized T1 controller that must be configured for ISDN. The router must connect to one of the following switch types: A 4 Electronic Switching System (4ESS), a DMS250, a DMS100, or a national ISDN (NI).

To configure ISDN NFAS, use the controller configuration-mode commands shown in the “ISDN NFAS Configuration Commands” table.

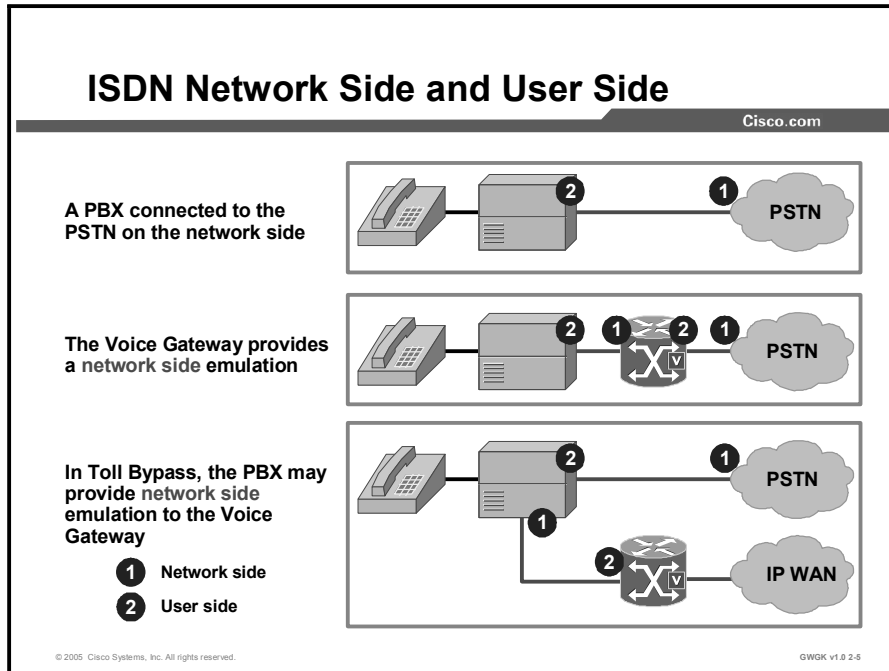
### ISDN NFAS Configuration Commands

| Command                                                                                              | Purpose                                                                                                                  |
|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <code>pri-group timeslots 1-24 nfas d<br/>primary nfas interface number<br/>nfas_group number</code> | On one channelized T1 controller, configure the NFAS primary D channel.                                                  |
| <code>pri-group timeslots 1-24 nfas d<br/>backup nfas interface number<br/>nfas_group number</code>  | On a different channelized T1 controller, configure the NFAS backup D channel to be used if the primary D channel fails. |
| <code>pri-group timeslots 1-24 nfas d none<br/>nfas interface number nfas group<br/>number</code>    | On other channelized T1 controllers, configure a 24 B-channel interface. (Optional)                                      |

An example of NFAS configuration is available at [http://www.cisco.com/warp/public/793/access\\_dial/quadt1\\_nfas.html#2](http://www.cisco.com/warp/public/793/access_dial/quadt1_nfas.html#2).

# Network Side vs. User Side

This topic describes the types of ISDN signaling switches used on the network and user sides.

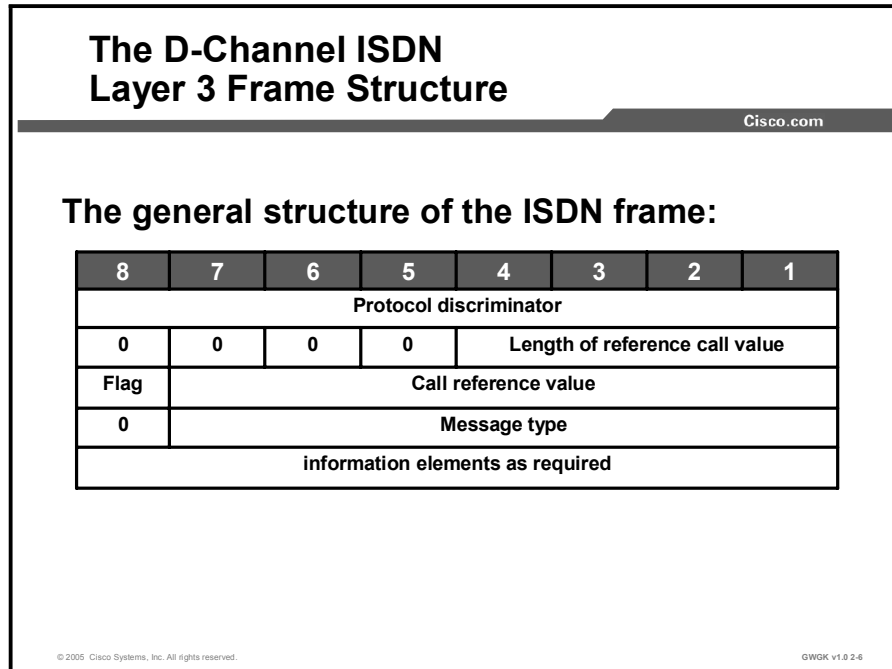


With ISDN connections, one end is subordinate to the other in a master-to-slave relationship. The master end is the network side of the connection and is known as the network termination (NT). The slave end is the user side of the connection and is known as the terminal equipment (TE). This type of relationship between network nodes is used to resolve conflicts that might exist when two endpoints in a call request the same thing, and only one of the two can gain access to the resource at a time. In this course, the NT device provides network-side connection while the TE device is the user-side connection. Typically, the responsibility for system clocking is assigned to the network side of a connection.

Network-side operation for these ISDN basic-rate and primary-rate switch types is supported by Net5, Net3, Q Signaling (QSIG), NI, 5ESS, and DMS100. Switch types are discussed in detail in the "Common ISDN Implementation Requirements" section.

# ISDN Signaling

This topic describes how ISDN passes messages on the D channel.



Because ISDN message types may influence the function of a BRI or PRI trunk configuration, it is important to examine the messages that are part of the Q.931 packet structure and see how ISDN carries out the signaling function.

ISDN signaling takes place in the D channel and uses a message-oriented protocol that supports call control signaling and packet data. In its role as signal carrier for the B channels, the D channel directs the central office (CO) switch to send incoming calls to particular timeslots on the Cisco access server or router.

The components of the ISDN frame that transmits these instructions are described as follows:

- **Protocol discriminator:** This is the protocol used to encode the remainder of the layer.
- **Length of call reference value:** This defines the length of the next field. The call reference may be one or two octets long depending on the size of the value being encoded.
- **Flag:** This is set to zero for messages sent by the party that allocated the call reference value; otherwise, it is set to one.
- **Call reference value:** This is an arbitrary value that is allocated for the duration of the specific session. This value identifies the call between the device maintaining the call and the ISDN switch.
- **Message type:** This identifies the message type (for example, SETUP) that determines what additional information is required and allowed. The message type may be one or more octets. When there is more than one octet, the first octet is coded as eight zeros.
- **ISDN information elements (IEs):** Most D-channel messages include additional information needed for call processing, such as the calling party number, called party number, and channel ID. The additional information in a message is passed in IEs. IEs are described in the “ISDN IEs” topic in this lesson.

## Most Common ISDN Message Types

Cisco.com

| 000 Call Establishment |                     | 001 Call Information |                     |
|------------------------|---------------------|----------------------|---------------------|
| 00001                  | ALERTing            | 00000                | USER INFOrmation    |
| 00010                  | CALL PROCeeding     | 00001                | SUSPend REJect      |
| 00011                  | PROGress            | 00010                | RESume REJect       |
| 00101                  | SETUP               | 00101                | SUSPend             |
| 00111                  | CONNect             | 00110                | RESume              |
| 01101                  | SETUP ACKnowledge   | 01101                | SUSPend ACKnowledge |
| 01111                  | CONNect ACKnowledge | 01110                | RESume ACKnowledge  |
| 010 Call Clearing      |                     | 011 Miscellaneous    |                     |
| 00101                  | DISConnect          | 00000                | SEGment             |
| 00110                  | Restart             | 00010                | FACility            |
| 01101                  | RELease             | 01110                | NOTIFY              |
| 01110                  | Restart ACKnowledge | 10101                | STATUS ENQuiry      |
| 11010                  | RELease COMplete    | 11001                | Congestion Control  |
|                        |                     | 11011                | INFORMATION         |
|                        |                     | 11101                | STATUS              |

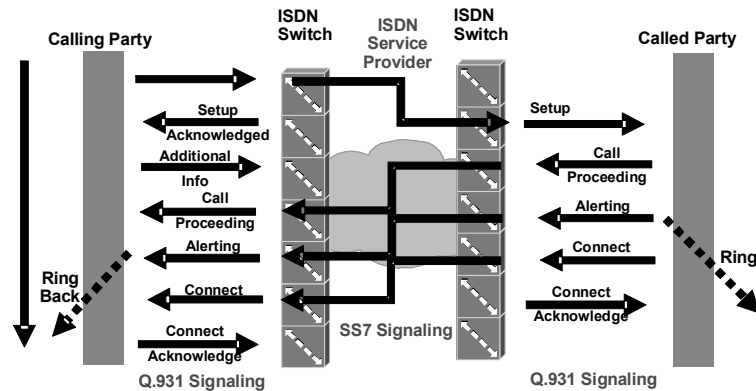
© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0 2-7

ISDN signaling is carried out by messages that are sent between endpoints on the D channel. The most common messages are listed in the figure above.

## ISDN D-Channel Message Flow

Cisco.com



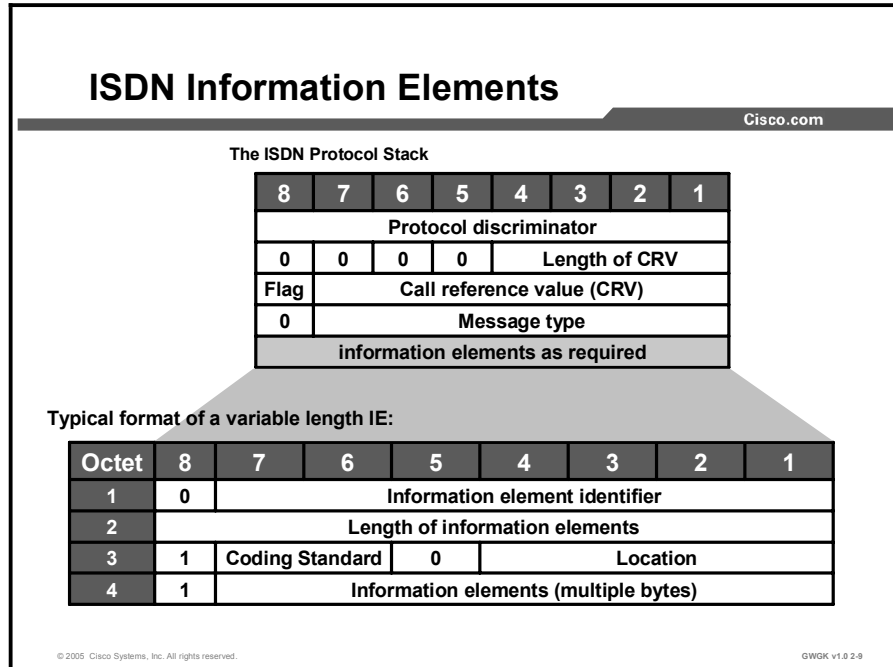
© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0 2-8

A simple Q.931 message exchange might progress as shown in the figure. Compare the call flow to the message types listed in the message type table in the previous figure.

# ISDN IEs

This topic describes information elements in ISDN signaling and how they are used by endpoints.



ISDN sends instructions in Layer 3 messages that are put into Layer 2 frames and are finally time-multiplexed onto a medium with either a BRI or a PRI Layer 1 linecoding specification.

A depiction of D-channel messages is shown in the figure. These messages allow complete control over call establishment and clearing, network maintenance, and the passing of other call-related information between switches.

The additional information required by an ISDN message is passed in IEs and varies depending on the message type, the action being performed, and the connected equipment. Mandatory and optional IEs for D-channel messages are defined in ITU-T Q.931.

IEs can be a single byte or several bytes, and by reading the message, the switch can determine this information. For example, in octet 1 of the IE, if bit 8, or the extension bit, is 0, the IE is of a variable length. If the bit is 1, the IE is a single byte.

The information contained in octet 3 is the coding standard and the location. The possible content of these fields is provided in the “Coding Standard” and “Location” tables.

### Coding Standard

| Bit Sequence | Meaning                             |
|--------------|-------------------------------------|
| 00           | ITU standardized coding             |
| 11           | Standard specific to location field |

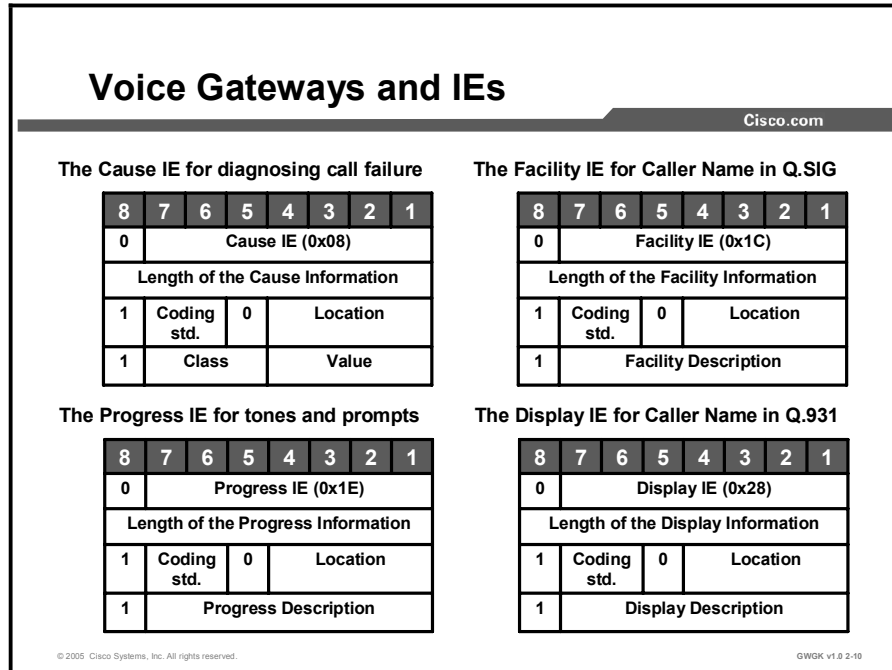
## Location

| Bit Sequence | Meaning                               |
|--------------|---------------------------------------|
| 0000         | User                                  |
| 0001         | Private network serving location user |
| 0010         | Public network serving local user     |
| 0011         | Transit network                       |
| 0100         | Public network serving remote user    |
| 0101         | Remote private network                |
| 0111         | International network                 |
| 1010         | Network beyond interworking point     |



## Example: IE in Action

A called number is passed to the PSTN by an IE. The IE contains bytes describing the numbering plan and the type of number. Typically, numbering type is not changed; however, there may be times when a network administrator may elect to have a specific gateway handle all the international calls. If this connection to the PSTN is an ISDN PRI, the IE must tell the PSTN that the called number is in international format.



A study of all available IEs is beyond the scope of this course. Commonly used IEs are listed in the in the “ISDN Progress Description Field Values” table. For further details, there are many public references available on the Internet. For this lesson, the cause, facility, progress, and display IEs are reviewed. They represent the information most in-demand in telephony systems and, therefore, most important in the communication between the voice gateway and PBX or PSTN.

### The Cause IE

The cause IE provides one or more octets that may help in diagnosing network or customer premises equipment (CPE) problems. When there is an ISDN problem in the network, a cause value, shown in octet 4 in the figure, is generated by the network and appears in the ISDN protocol log. The telephone company equipment translates these values to associated phrases. Cause messages are classified as normal events, resource or service availability, message validity, protocol error, or interworking. The most common phrases are listed in the following “Common IEs” table.

## The Facility IE

Supplemental services are invoked by sending facility IEs in a facility message to an ISDN switching device such as a PBX.

Supplemental services are widely used by PBXs and in the PSTN. IP telephony systems that are connected to these types of switches must be able to send and receive these messages. The supplemental service and associated parameters that are invoked are PBX-specific and should be provided by the PBX manufacturer.

## The Progress IE

Progress tones such as ringback and busy tones, and announcements such as “The number you have dialed is no longer in service,” are required to successfully signal voice calls. Progress tones can be generated by the originating, terminating, or intermediate devices.

The indication of in-band tones and announcements is controlled by the progress IE in ISDN and H.323 networks. The progress IE signals those interworking situations where in-band tones and announcements must be used.

The indication that tones and announcements are available is signaled by an alerting, call proceeding, progress, connect, setup acknowledge, or disconnect message containing a PI = 1 or 8, which would be sent in the progress description field in octet 4.

A SETUP message of PI = 3 means that the switch is indicating to the originating gateway that in-band messages are expected.

### ISDN Progress Description Field Values

| Hex Value | Decimal | Binary   | Description                                              |
|-----------|---------|----------|----------------------------------------------------------|
| 0x01      | 1       | 000 0001 | Call is not end-to-end ISDN                              |
| 0x02      | 2       | 000 0010 | Destination address is non-ISDN                          |
| 0x03      | 3       | 000 0011 | Origination address is non-ISDN                          |
| 0x04      | 4       | 000 0100 | Call has returned to the ISDN                            |
| 0x08      | 8       | 000 1000 | In-band information or appropriate pattern now available |
| 0x0A      | 10      | 000 1010 | Delay in response at destination interface               |

## The Display IE

The display IE sends text to do such things as provide output for an LCD display. This IE is commonly used to pass calling name information over PRI, although there are PBXs and telecommunications service providers with NI3-type ISDN switches that only pass calling name information with the facility IE in Q.SIG. The display and facility IEs are used by Cisco CallManager to support caller name and number identification presentation. These services are based on the device control protocols that handle the call. Not all device protocols provide caller number and name information in the protocol messages.

## Common IEs

| Value | Name                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                          |
|-------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| 0x04  | Bearer                                     | Specifies packet or circuit mode, data rate, type of information content (voice)                                                                                                                                                                                                                                                                                                                                                          |                                                          |
| 0x08  | Cause                                      | This IE provides the reason a call was rejected or disconnected. A sample of possible causes are as follows:                                                                                                                                                                                                                                                                                                                              |                                                          |
|       |                                            | 0x01                                                                                                                                                                                                                                                                                                                                                                                                                                      | Unassigned number                                        |
|       |                                            | 0x03                                                                                                                                                                                                                                                                                                                                                                                                                                      | No route to destination                                  |
|       |                                            | 0x06                                                                                                                                                                                                                                                                                                                                                                                                                                      | Channel unacceptable                                     |
|       |                                            | 0x10                                                                                                                                                                                                                                                                                                                                                                                                                                      | Normal call clearing                                     |
|       |                                            | 0x11                                                                                                                                                                                                                                                                                                                                                                                                                                      | User busy                                                |
|       |                                            | 0x12                                                                                                                                                                                                                                                                                                                                                                                                                                      | User not responding                                      |
|       |                                            | 0x13                                                                                                                                                                                                                                                                                                                                                                                                                                      | User alerting; no answer                                 |
|       |                                            | 0x1B                                                                                                                                                                                                                                                                                                                                                                                                                                      | Destination out of order                                 |
|       |                                            | 0x1C                                                                                                                                                                                                                                                                                                                                                                                                                                      | Invalid number format                                    |
|       |                                            | 0x22                                                                                                                                                                                                                                                                                                                                                                                                                                      | No circuit or channel available                          |
| 0x2A  | Switching equipment congestion             |                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                          |
| 0x14  | Call State                                 | The current status of a call in terms of the standard Q.931 state machine                                                                                                                                                                                                                                                                                                                                                                 |                                                          |
| 0x18  | Channel ID                                 | Defines the B channel being used                                                                                                                                                                                                                                                                                                                                                                                                          |                                                          |
| 0x1C  | Facility                                   | <p>The purpose of the facility IE is to indicate the invocation and operation of supplemental services, identified by the corresponding operation value within the facility IE. Examples of supplemental services are as follows:</p> <ul style="list-style-type: none"> <li>■ Called or calling party identification</li> <li>■ Subaddressing</li> <li>■ Hold or retrieve</li> <li>■ Call transfer</li> <li>■ Message waiting</li> </ul> |                                                          |
| 0x1E  | Progress Indication                        | This IE provides information about the call in progress. Progress indication examples are as follows:                                                                                                                                                                                                                                                                                                                                     |                                                          |
|       |                                            | 0x01                                                                                                                                                                                                                                                                                                                                                                                                                                      | Call is not end-to-end ISDN                              |
|       |                                            | 0x02                                                                                                                                                                                                                                                                                                                                                                                                                                      | Destination address is non-ISDN                          |
|       |                                            | 0x03                                                                                                                                                                                                                                                                                                                                                                                                                                      | Origination address is non-ISDN                          |
|       |                                            | 0x04                                                                                                                                                                                                                                                                                                                                                                                                                                      | Call has returned to the ISDN                            |
|       |                                            | 0x08                                                                                                                                                                                                                                                                                                                                                                                                                                      | In-band information or appropriate pattern now available |
| 0x0A  | Delay in response at destination interface |                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                          |
| 0x28  | Display                                    | This IE provides human-readable text that can be specified with almost any message (for example, to provide text for an LCD display).                                                                                                                                                                                                                                                                                                     |                                                          |
| 0x2C  | Keypad                                     | Dialed digits                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                          |
| 0x34  | Signal                                     | Provides call status tones according to the following chart:                                                                                                                                                                                                                                                                                                                                                                              |                                                          |
|       |                                            | 0x00                                                                                                                                                                                                                                                                                                                                                                                                                                      | Dial tone                                                |

| Value | Name                 | Description                                                                       |                                |                                                             |
|-------|----------------------|-----------------------------------------------------------------------------------|--------------------------------|-------------------------------------------------------------|
|       |                      | 0x01                                                                              | Ringling                       | 440 Hz + 480 Hz; 2 sec on/4 sec off                         |
|       |                      | 0x02                                                                              | Intercept                      | Alternating 440 Hz and 620 Hz; 250 ms                       |
|       |                      | 0x03                                                                              | Network congestion (fast busy) | 480 Hz + 620 Hz; 250 ms on/250 ms off                       |
|       |                      | 0x04                                                                              | Busy                           | 480 Hz + 620 Hz; 500 ms on/500 ms off                       |
|       |                      | 0x05                                                                              | Confirm                        | 350 Hz + 440 Hz; repeated three times: 100 ms on/100 ms off |
|       |                      | 0x06                                                                              | Answer                         | not used                                                    |
|       |                      | 0x07                                                                              | Call waiting                   | 440 Hz; 300 ms burst                                        |
|       |                      | 0x08                                                                              | Off-hook warning               | 1400 Hz + 2060 Hz + 2450 Hz + 2600 Hz; 100 ms on/100 ms off |
|       |                      | 0x3F                                                                              | Tones                          | off                                                         |
| 0x3A  | SPID                 | Contains a service profile identifier (SPID)                                      |                                |                                                             |
| 0x4C  | Connected Number     | If a disconnect occurs during CONFERENCE, this IE indicates the remaining caller. |                                |                                                             |
| 0x6C  | Calling Party Number | The origin phone number                                                           |                                |                                                             |
| 0x70  | Called Party Number  | The phone number being dialed                                                     |                                |                                                             |
| 0x7C  | LLC                  | Lower layer compatibility                                                         |                                |                                                             |
| 0x7D  | HLC                  | Higher layer compatibility                                                        |                                |                                                             |
| 0x7E  | User-User            | User-user information                                                             |                                |                                                             |

## Example: IEs in Action

Cisco.com

```
*Mar 27 15:11:40.472: ISDN Se0/0:23 Q931: TX -> SETUP pd = 8 callref = 0x0006
 Bearer Capability i = 0x8090
 Standard = CCITT
 Transer Capability = Speech
 Transfer Mode = Circuit
 Transfer Rate = 64 kbit/s
 Channel ID i = 0xA98397
 Exclusive, Channel 23
 Calling Party Number i = 0x2181, 'XXXXXXXXXX'
 Plan:ISDN, Type:National
 Called Party Number i = 0x80, 'XXXXXXXXXX'
 Plan:Unknown, Type:Unknown
*Mar 27 15:11:40.556: ISDN Se0/0:23 Q931: RX <- CALL_PROC pd = 8 callref = 0x8006
 Channel ID i = 0xA98397
 Exclusive, Channel 23
*Mar 27 15:11:42.231: ISDN Se0/0:23 Q931: RX <- PROGRESS pd = 8 callref = 0x8006
 Progress Ind i = 0x8488 - In-band info or appropriate now available
*Mar 27 15:11:45.697: ISDN Se0/0:23 Q931: TX -> DISCONNECT pd = 8 callref = 0x0006
 Cause i = 0x8090 - Normal call clearing
*Mar 27 15:11:45.733: ISDN Se0/0:23 Q931: RX <- RELEASE pd = 8 callref = 0x8006
*Mar 27 15:11:45.757: ISDN Se0/0:23 Q931: TX -> RELEASE_COMP pd = 8 callref = 0x0006
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK v1.0-2.11

There are several sources available on Cisco.com to help read the output, including the meaning of the hexadecimal values, from a **debug isdn q931** command. Refer to the following sources:

- The “ISDN Codes” chapter in the *Debug Command Reference* at [http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products\\_command\\_reference\\_chapter09186a008007ff75.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_command_reference_chapter09186a008007ff75.html).
- The **debug isdn q931** command in the *Debug Command Reference* at [http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products\\_command\\_reference\\_chapter09186a008007ff85.html#xtocid90247](http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_command_reference_chapter09186a008007ff85.html#xtocid90247).
- For hexadecimal values, refer to Table 2-53 in the *Debug Command Reference* [http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products\\_command\\_reference\\_chapter09186a008007ff85.html#23059](http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_command_reference_chapter09186a008007ff85.html#23059).

The “ISDN Bearer Capability Values” table, taken from the *Debug Command Reference* cited previously, provides an example of how to read the hexadecimal values with the ISDN bearer capability values.

## ISDN Bearer Capability Values

| Field | Value Description                                         |
|-------|-----------------------------------------------------------|
| 0x    | Indication that the values that follow are in hexadecimal |
| 88    | ITU-T coding standard; unrestricted digital information   |
| 90    | Circuit mode, 64 kbps                                     |
| 21    | Layer 1, V.110/X.30                                       |
| 8F    | Synchronous, no in-band negotiation, 56 kbps              |

You are also told that 0x8890 is for 64 kbps or 0x8890218F for 56 kbps. The SETUP message in the example configuration in the figure indicates that **Bearer Capability I = 0x8890**. Therefore, you know that you have a 64kbps bearer stream.

The sample output in the figure shows Cause i = 8090, which is translated as normal call clearing. A different cause code, such as Cause i = 829F, is shown in the “ISDN Cause Codes Fields” table in the “ISDN Codes” chapter of the *Debug Command Reference*. The table shows that i = 0x y1 y2 z1 z2 [a1 a2]. The following provides values for y1, y2, z1, and z2:

- y1 = 8, which refers to ITU-T standard coding
- y2 = 2, which refers to public network serving local user
- z1 and z2 combine to form 9F, which, in decimal is 160 or in binary is 10011110. Removing the most significant bit leaves 0011110, or decimal 31, which is 0x1F. Compare this to the “Excerpt from the ISDN Cause Values” table taken from the *Debug Command Reference*. Decimal 31 or 1F translates to a normal, unspecified cause with the explanation that this value reports the occurrence of a normal event when no standard cause applies. No action is required.

#### Excerpt from the ISDN Cause Values

| Decimal | Hexadecimal | Cause                        | Explanation                                                                                           |
|---------|-------------|------------------------------|-------------------------------------------------------------------------------------------------------|
| 30      | 1E          | Response to STATUS ENQUIRY   | The status message was generated in direct response to the prior receipt of a status enquiry message. |
| 31      | 1F          | Normal, unspecified          | Reports the occurrence of a normal event when no standard cause applies. No action required.          |
| 34      | 22          | No circuit/channel available | The connection cannot be established because no appropriate channel is available to take the call.    |

The table shows that the disconnection specified in this cause code is that the PSTN connection disconnected for some normal reason for which no other information is provided.

The “Most Common Message Types and Associated IEs” table provides a list of message types and the IEs that can be associated with each message.

## Most Common Message Types and Associated IEs

| Message Type        | IEs Associated with Message                                                                                                                                                                                                                                                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ALERTing            | Bearer capability, Channel identification, Progress indicator, Display, Signal, Higher layer compatibility                                                                                                                                                                                                                                                         |
| CALL PROCeeding     | Bearer capability, Channel identification, Progress indicator, Display, Higher layer compatibility                                                                                                                                                                                                                                                                 |
| SETUP               | Sending complete, Repeat indicator, Bearer capability, Channel identification, Progress indicator, Network specific facilities, Display, Keypad facility, Signal, Calling party number, Calling party subaddress, Called party number, Called party subaddress, Transit network selection, Repeat indicator, Lower layer compatibility, Higher layer compatibility |
| CONNect             | Bearer capability, Channel identification, Progress indicator, Display, Date/time, Signal, Lower layer compatibility, Higher layer compatibility                                                                                                                                                                                                                   |
| SETUP ACKnowledge   | Channel identification, Progress indicator, Display, Signal                                                                                                                                                                                                                                                                                                        |
| CONNect ACKnowledge | Display, Signal                                                                                                                                                                                                                                                                                                                                                    |
| DISConnect          | Cause, Progress indicator, Display, Signal                                                                                                                                                                                                                                                                                                                         |
| RELease             | Cause, Display, Signal                                                                                                                                                                                                                                                                                                                                             |
| RELease COMplete    | Cause, Display, Signal                                                                                                                                                                                                                                                                                                                                             |
| STATUS ENQuiry      | Display                                                                                                                                                                                                                                                                                                                                                            |
| STATUS              | Cause, Call state, Display                                                                                                                                                                                                                                                                                                                                         |



# ISDN Numbering Plan

This topic describes how to select and configure the correct ISDN numbering plan.

## ISDN Numbering Plans

Cisco.com

```
*Mar 27 15:11:40.472: ISDN Se0/0:23 Q931: TX -> SETUP pd = 8 callref = 0x0006
 Bearer Capability i = 0x8090A2
 Standard = CCITT
 Transfer Capability = Speech
 Transfer Mode = Circuit
 Transfer Rate = 64 kbit/s
 Channel ID i = 0xA98397
 Exclusive, Channel 23
 Calling Party Number i = 0x2181, 'XXXXXXXXXX'
 Plan:ISDN, Type:National
 Called Party Number i = 0x80, 'XXXXXXXXXX'
 Plan:Unknown, Type:Unknown
```

- To meet service provider numbering type requirements, and other call routing requirements the numbering-type dial-peer option can be used
- numbering-type matching works in conjunction with the existing parameter such as incoming called-number, answer-address and destination-pattern
- Some service providers require specific numbering types for certain calls. For example AT&T 4ESS requires international calls to be flagged as international numbering type

© 2005 Cisco Systems, Inc. All rights reserved. GWOK v1.0 2-12

The numbering plan, and a field called numbering type, are contained in the calling and called party number IEs. This information is highlighted for a PRI in the **debug q931** command output in the figure. In the majority of cases, these fields are ignored by most ISDN switches. However, there are times when ISDN switches base their call routing decision partially on the numbering plan or type. PBXs also use the calling party numbering plan information for number-presentation purposes. Numbering type allows dial-peer matching. To use the numbering-type feature, dial peers must be configured for called number, answer number, or destination pattern.

To match on a number type for a dial-peer call leg, use the **numbering-type** command in dial-peer configuration mode. To remove the numbering type for a dial-peer call leg, use the **no** form of this command. For example, in a PBX-centric voice network, international calls may be routed out to a dedicated international gateway instead of to a domestic gateway. To handle international calls this way, the international number is routed to a gateway with numbering-type dial-peer matching. In another example, a local PSTN ISDN provider may have an older switch that reads some national calls as international and sends them to the long-distance carrier. To tell the local ISDN switch that the calls are domestic, the gateway should be configured to pass on the numbering type as “national”.

The following is an example of the **numbering-type** command as it resides under the dial-peer voice:

```
dial-peer voice 100 voip
 numbering-type national
 destination-pattern 91408.....
 prefix 1408
 port 1/0:23

dial-peer voice 101 POTS
 numbering-type international
 destination-pattern 9011T
 prefix 011
 port 1/0:23
```

### numbering-type Command Syntax Description

| Numbering Plan Indicator | Description                                  |
|--------------------------|----------------------------------------------|
| international            | Specifies international numbering type       |
| abbreviated              | Specifies abbreviated numbering type         |
| national                 | Specifies national numbering type            |
| network                  | Specifies network numbering type             |
| reserved                 | Specifies reserved numbering type            |
| subscriber               | Specifies subscriber numbering type          |
| unknown                  | Specifies that the numbering type is unknown |

For MGCP gateways, Cisco CallManager sets the calling-directory number type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans, such as with the North American Numbering Plan (NANP) or with European dialing plans. You may need to change the defaults in Europe because Cisco CallManager does not recognize all European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory numbering plan type.

The Cisco CallManager supports the following called and calling party IE number type options:

- **Cisco CallManager:** The Cisco CallManager sets the directory type.
- **Unknown:** This option specifies that the dialing plan is unknown.
- **National:** Use this type when you are dialing within the dialing plan for your country.
- **International:** Use this type when you are dialing outside the dialing plan for your country.
- **Subscriber:** Use this type for site-specific dial plans set by the PSTN subscriber.

# Common ISDN Implementation Requirements

This topic describes common ISDN issues when deploying a gateway.

## Common ISDN Implementation Requirements

Cisco.com

- **Obtain correctly provisioned service**
- **Switch type**
- **System clocking**
- **ISDN timers**
- **Calling Name Display**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0 2-13

The key requirements for an ISDN gateway deployment are as follows:

- Obtain a correctly provisioned ISDN PRI line from a telecommunications service provider.
- The service provider should specify the switch type that needs to be configured.
- A common clock source must be used between devices.
- ISDN timers are used to clear calls following defined periods of inactivity and are set to improve the efficiency of network resource consumption.

## Correctly Provisioned Service

Cisco.com

**Step 1: Verify if the outgoing B channel calls are made in ascending or descending order.**

**Step 2: Ask for delivery of calling line identification.**

**Step 3: Request PRI switch configuration attributes.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-14

Before configuring ISDN PRI on a Cisco router, a correctly provisioned ISDN PRI line is required from a telecommunications service provider. The process of provisioning a PRI varies dramatically from provider to provider on a national and international basis. However, there are some general guidelines described as follows:

- Step 1**     Verify if the outgoing B-channel calls are made in ascending or descending order. The default in Cisco IOS software is descending order. However, if the service-provider switch is configured for outgoing calls made in ascending order, the router can be configured to match the service-provider switch configuration.
- Step 2**     Ask for delivery of calling line ID (CLID). Providers sometimes call this automatic number identification (ANI).
- Step 3**     When ordering ISDN service, request the PRI switch configuration attributes, which are displayed in the following “PRI Switch Configuration Attributes” table.

## PRI Switch Configuration Attributes

| Attribute                              | Configuration Attributes for 5ESS, DMS100, and 4ESS                      |
|----------------------------------------|--------------------------------------------------------------------------|
| Line format                            | Extended Superframe (ESF) format                                         |
| Line coding                            | Binary 8-zero substitution (B8ZS)                                        |
| Call type                              | 23 incoming channels and 23 outgoing channels                            |
| Speed                                  | 64 kbps                                                                  |
| Call-by-call capability                | Enabled                                                                  |
| Channels                               | 23 B + D                                                                 |
| Trunk selection sequence               | Either ascending order (from 1 to 23) or descending order (from 23 to 1) |
| B + D glare                            | Yield                                                                    |
| Directory numbers                      | Only one directory number assigned by service provider                   |
| ISDN call speed outside local exchange | Speed set to 56 kbps outside local exchange                              |
| SPIDs required?                        | None                                                                     |

## Switch Type

Cisco.com

- **The correct version must be specified so that the voice gateway can communicate with the service provider ISDN switch or with the PBX.**
- **The service provider should specify the switch type. Occasionally the switch type will be one of the following:**
  - **Custom**
  - **National**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2-15

Q.931 comes in many local versions, so the correct version must be specified for the voice gateway to communicate with the service-provider ISDN switch or with the PBX.

The service provider should specify the switch type that needs to be configured. Occasionally, the switch type is “custom” or “national”, in which case the following guidelines apply:

- **Custom:** Configure the switch type on the router as **basic-5ess** for a BRI with a 5ESS switch, **primary-5ess** for a PRI with 5ESS, **basic-dms** for a BRI with a DMS switch, or **primary-dms** for PRI with DMS.
- **National:** Configure the switch type on the router as **basic-ni** for BRI or **primary-ni** for PRI.

---

**Note** For Cisco IOS Software Releases up to 11.2, configuration of the ISDN switch type is a global command and is not configurable on the interface. This restriction prevents BRI and PRI interface cards from being deployed in the same chassis. In Cisco IOS Software Release 11.3T and later, multiple switch types in a single Cisco IOS chassis are supported.

---

Once the service provider specifies the switch type, use the **isdn switch-type** command to configure it on the router as follows:

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#isdn switch-type basic-5ess
Router(config)#exit
```

## System Clocking

Cisco.com

- **If a common clock source is not used between devices, the binary values in the bit streams may be misinterpreted.**
- **PSTN switches may serve several organizations.**
- **Where clocking must be explicitly configured, use Cisco IOS software commands in global configuration mode:**
  - `network-clock-participate [slot slot-number | wic wic-slot | aim aim-slot-number]`
  - `network-clock-select priority {t1 | e1} slot/port`

© 2005 Cisco Systems, Inc. All rights reserved.

QWQK v1.0 2-16

If a common clock source is not used between devices, the binary values in the bit streams may be misinterpreted because the device samples the signal at the wrong moment. For example, if the local timing of a receiving device is using a slightly shorter time period than the timing of the sending device, a string of eight continuous binary 1s may be interpreted as 9 continuous 1s. If this data is then resent to further downstream devices that use different timing references, the error could be compounded. When each device in the network uses the same clocking signal, the integrity of the traffic across the entire network is ensured.

PSTN switches may serve several organizations and will be set to provide clocking to devices that connect to them. In the case of a voice gateway that is inserted between a PBX and the PSTN, the gateway takes its clocking from the PSTN and in turn provides clocking to the PBX. Cisco documentation says that system clocking can be set by establishing the network side of a connection. In cases where clocking must be explicitly configured, the internal propagation of system clocking is handled by these Cisco IOS software commands in the global configuration mode:

- To allow the ports on a specified network module or voice WAN interface card (VWIC) to use the network clock for timing, use **network-clock-participate** `[slot slot-number | wic wic-slot | aim aim-slot-number]`.
- To name a source to provide timing for the network clock and to specify the selection priority for this clock source, use **network-clock-select** `priority {t1 | e1} slot/port`.

## ISDN Timers

Cisco.com

- **ISDN timers clear calls following defined periods of inactivity and can be set to improve the efficiency of network resource consumption.**
- **ISDN timers are configured at the interface. The T306 timer is designed for routers that are configured as an ISDN network-side switch.**
- **When a data link layer malfunction occurs, calls that are not in the active state are cleared. For calls that are not in the active state, the T309 timer is started.**
- **The T310 timer starts when a router receives a call proceeding message; it stops when the call exits the call proceeding state.**
- **The T321 timer must be implemented when you use the D channel backup procedure involving D channel switchover.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0 2-17

ISDN timers clear calls following defined periods of inactivity and can be set to improve the efficiency of network resource consumption. ISO defines all the Layer 2 and Layer 3 timers. A sample of the types of timers is listed in the “ISO Layer 3 ISDN Timers” table. All the ISDN timers are configurable, but T306, T309, T310, and T321 are more important for correct operation.

ISDN timers are configured at the interface with a command such as the **isdn t306 msec** command. The T306 timer is designed for routers that are configured as an ISDN network-side switch. When a router receives a disconnect message with a progress indicator of 8, it disconnects the call after waiting for the specified number of milliseconds while the in-band announcement or error tone is playing. Be sure to set the timer long enough for the announcement to be heard or the tone to be recognized. This command is used only for disconnect messages with a progress indicator of 8; otherwise, the T305 timer is used. The **disable** and **no** forms of this command have the same result; the timer waits for the default number of milliseconds before disconnecting the call.

When a data-link layer malfunction occurs, calls that are not in the active state are cleared. For calls that are not in the active state, the T309 timer is started. The timer is stopped when the data link is reconnected. If the T309 timer expires prior to the reestablishment of the data link, the network clears the connection and call to the remote user, and it sends a disconnect cause of 27 to indicate that the call destination is out of order. The network releases and disconnects the B channel, and releases the call reference, to enter the null state. The T309 timer is mandatory for routers that are configured as an ISDN network-side switch, and by default the timer is set to expire after 90 ms. The implementation of the T309 timer is optional for the user side of the network. The **isdn timer t309** command is used for changing the value of the T309 timer.

The T310 timer starts when a router receives a call-proceeding message; it stops when the call exits the call-proceeding state, which typically occurs when the call moves to the alerting, connect, or progress state. If the timer expires while the call is in the call-proceeding state, the router releases the call. Set the timer to match the specific characteristics of your network.



The T321 timer must be implemented when you use the D-channel backup procedure involving D-channel switchover. The **isdn timer t321** command is used for changing the value of the T321 timer.

### ISO Layer 3 ISDN Timers

| Name | Started   | Stopped          | Notes                                                                                                                                                                                                                                                                                                  |
|------|-----------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T301 | ALERT     | CONNECT          | -                                                                                                                                                                                                                                                                                                      |
| T302 | SETUP     | SETUP_ACK        | Overlapped sending only                                                                                                                                                                                                                                                                                |
| T303 | SETUP     | CALL_PROC        | -                                                                                                                                                                                                                                                                                                      |
| T304 | SETUP     | SETUP_ACK        | -                                                                                                                                                                                                                                                                                                      |
| T305 | DISC      | RELEASE          | -                                                                                                                                                                                                                                                                                                      |
| T306 | DISC      | REL/DISC         | This timer is used for routers that are configured as an ISDN network-side switch. When a router receives a disconnect message with a progress indicator of 8, it disconnects the call after waiting for the specified number of milliseconds while the in-band announcement or error tone is playing. |
| T308 | RELEASE   | REL_COM          | -                                                                                                                                                                                                                                                                                                      |
| T309 | -         | -                | This timer indicates how long to keep B channels when D channels go down.                                                                                                                                                                                                                              |
| T310 | CALL_PROC | ALERT/CONNECT    | -                                                                                                                                                                                                                                                                                                      |
| T314 | -         | -                | Segmentation                                                                                                                                                                                                                                                                                           |
| T316 | RESTART   | RESTART_ACK/REJ  | -                                                                                                                                                                                                                                                                                                      |
| T317 | -         | -                | -                                                                                                                                                                                                                                                                                                      |
| T318 | RESUME    | RESUME_ACK/REJ   | -                                                                                                                                                                                                                                                                                                      |
| T319 | SUSPEND   | SUSPEND_ACK/REJ  | -                                                                                                                                                                                                                                                                                                      |
| T321 | -         | -                | D channel failure to restart attempts                                                                                                                                                                                                                                                                  |
| T316 | STATUS    | DISC/REL/REL_COM | -                                                                                                                                                                                                                                                                                                      |

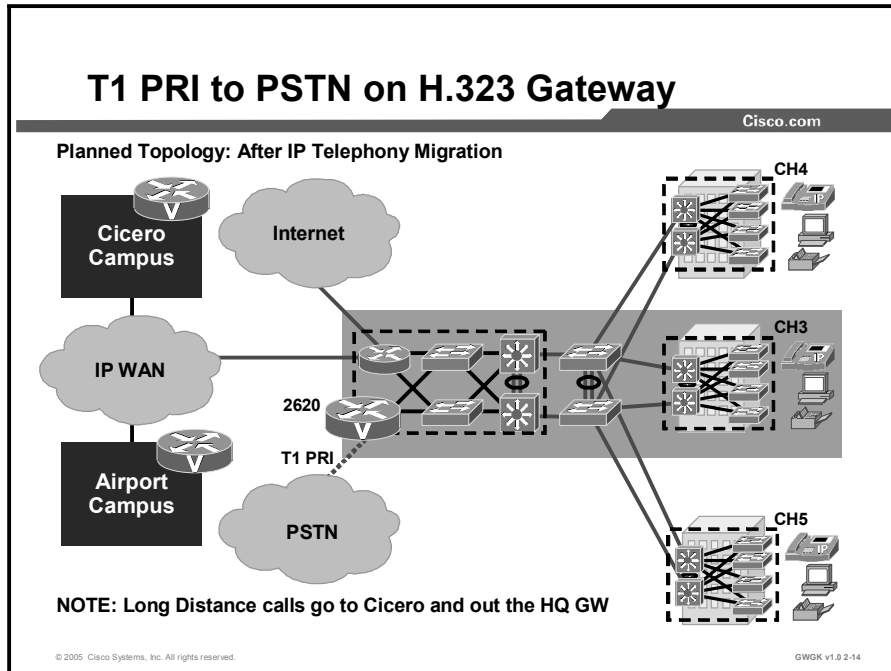
## Calling Name Display

Cisco CallManager, with either an H.323 or an MGCP gateway, supports any device sending calling party name information in a display IE, but not in a facility IE.

With ISDN calling name display feature for SIP gateways in Cisco IOS 12.3 T (4), SIP signaling on Cisco IOS gateways has been enhanced to update the calling name and number information in SIP headers as per the recommended SIP standards. Also included is the complete translation of ISDN screening and presentation indicators, which allows SIP customers basic caller ID privileges. Configuration instructions are available at [http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/calle\\_c/sip\\_c/sipc1\\_c/chapter9.htm#wp1063971](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_c/sip_c/sipc1_c/chapter9.htm#wp1063971).

# Common ISDN Gateway Configuration Examples

This topic describes how to configure a gateway to support ISDN connections.



The figure shows the Woodridge campus of Span Engineering. A T1 PRI has been ordered from the telephone company and has been installed. An H.323 voice gateway will be deployed on a Cisco 2620 platform with a High-Density Voice Network Module (HDV-NM) and a T1 Multiflex Trunk VWIC (VWIC-1MFT-T1). The “Configuring PRI Interfaces” table provides the steps required to configure a PRI on a voice gateway.

## Configuring PRI Interfaces

| Step | Action                                                                                                                                                                                                                                                                                                                       | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | <code>Router(config)#isdn switch-type switch-type</code>                                                                                                                                                                                                                                                                     | Configures the global ISDN switch type to match the service provider switch type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 2.   | <pre>Router(config)#controller t1 1/0 or Router(config)#controller e1 1/0</pre> While in controller configuration mode, configure framing, linecode and timeslots: <pre>Router(config-controller)#framing esf Router(config-controller)#linecode{ami   b8zs   hdb3} Router(config-controller)#pri-group timeslots 1-23</pre> | Configures the T1 or E1 controller <ul style="list-style-type: none"> <li>■ <b>Framing</b> defines framing characteristics, such as Superframe (SF) or ESF</li> <li>■ <b>Linecoding:</b> <ul style="list-style-type: none"> <li>— <b>ami:</b> Alternate mark inversion (AMI), valid for T1 or E1 controllers. Default for T1 lines.</li> <li>— <b>b8zs:</b> B8ZS, valid for T1 controllers only.</li> <li>— <b>hdb3:</b> High-density binary 3 (HDB3), valid for E1 controllers only. Default for E1 lines.</li> </ul> </li> <li>■ <b>pri-group timeslots:</b> The maximum T1 range is 1 to 23. The maximum E1 range is 1 to 31. Separate low and high values with a hyphen. The PRI group can include all the available timeslots or a select group of timeslots.</li> </ul> |
| 3.   | <code>Router(config-if)#isdn incoming-voice voice</code>                                                                                                                                                                                                                                                                     | Configures the port for incoming voice calls                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 4.   | <code>Router(config-if)#isdn-bchan-number-order {descending   ascending}</code>                                                                                                                                                                                                                                              | This command configures an ISDN PRI interface to make outgoing call selection in ascending or descending order. For example, the interface selects the lowest or highest available B channel starting at either channel B1 (ascending) or channel B23 for a T1 and channel B30 for an E1 (descending). The default is descending.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 5.   | <code>Router(config-if)#show running-configuration</code>                                                                                                                                                                                                                                                                    | Before configuring ISDN PRI on your router, check with your service vendor to determine if ISDN trunk call selection is configured for ascending or descending order. A mismatch between router and switch causes the switch to send an error message stating that the channel is not available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 6.   | Configure dial-peers                                                                                                                                                                                                                                                                                                         | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Complete instructions for the configuration of ISDN PRI voice-interface support can be found at

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/isdnv\\_c/isdn01.htm#wp1038644](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/isdnv_c/isdn01.htm#wp1038644).

## T1 PRI to PSTN on H.323 Gateway (Cont.)

Cisco.com

- **Step #1 – Define the ISDN switch type**

```
WDGRouter(config)#isdn switch-type primary-ni
WDGRouter(config)# network-clock-participate slot 1
WDGRouter(config)# network-clock-select 1 T1 1/0
```

- **Step #2 – Configure the T1 Controller**

```
WDGRouter(config)#controller t1 1/0
WDGRouter(config-controller)#framing esf
WDGRouter(config-controller)#linecode b8zs
WDGRouter(config-controller)#pri-group timeslots 1-24
WDGRouter(config-controller)#exit
```

- **Step #3 – Configure the Interface**

```
WDGRouter(config-if)#isdn incoming-voice voice
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0 2-15

The steps listed in the figure are shown in more detail here. These steps replicate what the user might expect to see when carrying out a configuration.

**Step 1** Since a T1 PRI is used in this example, it is necessary to define the ISDN switch type in the global configuration.

```
WDGRouter(config)#isdn switch-type ?
 primary-4ess AT&T 4ESS switch type for the U.S.
 primary-5ess AT&T 5ESS switch type for the U.S.
 primary-dms100 Northern Telecom switch type for the U.S.
 primary-net5 European switch type for NET5
 primary-ni National ISDN switch type
 primary-ntt Japan switch type
 primary-ts014 Australia switch type
WDGRouter(config)#isdn switch-type primary-ni
WDGRouter(config)# network-clock-participate slot 1
WDGRouter(config)# network-clock-select 1 T1 1/0
```

**Step 2** Configure the T1 controller for ISDN PRI signaling.

```
WDGRouter(config)#controller t1 1/0
!--- This is the first VWIC port on NM-HDV.
WDGRouter(config-controller)#framing esf
WDGRouter(config-controller)#linecode b8zs
WDGRouter(config-controller)#pri-group timeslots 1-24
!--- Defines the T1/PRI port for common channel signaling.
```

---

**Note** After configuring the **pri-group** command, the D channel (interface serial 1/0:23) and the voice port (voice-port 1/0:23) are created automatically by the router.

---

**Step 3** Configure the interface. The configuration of the PRI for incoming voice is shown in this example. This command is added automatically but is shown in the figure to show the sequence.

```
WDGRouter(config)#interface s1/0:23
WDGRouter(config-if)#isdn incoming-voice voice
```

## T1 PRI to PSTN on H.323 Gateway (Cont.)

Cisco.com

- **Step #4 –Verify the ISDN D-channel configuration.**

```
WDGRouter(config)# show running-configuration
interface Serial1/0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-ni
 !--- Switch-type takes precedence over the global.
 isdn incoming-voice voice
 !--- This defines incoming calls from PSTN as voice.
 no cdp enable
```

- **Step #5 – Configure dial peer statements**

```
WDGRouter(config)#dial-peer voice 1 pots
WDGRouter(config-dial-peer)#destination-pattern 9T
WDGRouter(config-dial-peer)#direct-inward-dial
WDGRouter(config-dial-peer)#port 1/0:23
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0 2-16

- Step 4** Verify the ISDN D-channel (interface serial 1/0:23) configuration. After completing Step 2, the **show running-configuration** command output should display the D-channel configuration as shown in this example.

```
interface Serial1/0:23
 !--- This is the D channel for PRI.
 no ip address
 no logging event link-status
 isdn switch-type primary-ni
 !--- This switch-type takes precedence over the global.
 isdn incoming-voice voice
 !--- This defines incoming calls from PSTN as voice.
 no cdp enable
```

---

**Note** The relevant command under the interface serial 1/0:23 configuration is **isdn incoming-voice voice**.

---

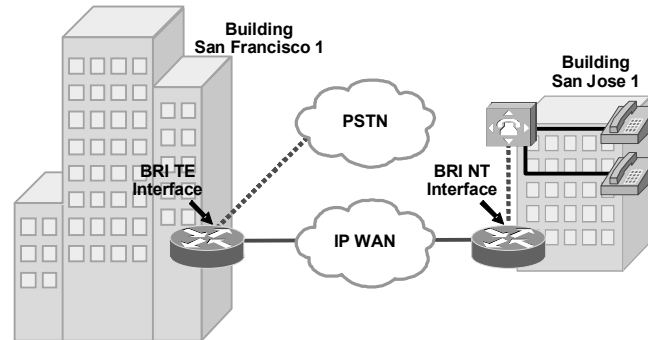
- Step 5** Configure dial-peer statements.

```
WDGRouter(config)#dial-peer voice 1 pots
!--- The dial peer is pointing to the PRI trunk to the PSTN.
WDGRouter(config-dial-peer)#destination-pattern 9T
!--- Route this pattern to the PSTN cloud through the T1/PRI.
!--- T is a wildcard for any digits.
WDGRouter(config-dial-peer)#direct-inward-dial
!--- Direct-inward-dial (DID) does not generate a secondary
!--- dialtone on incoming calls from PSTN.
WDGRouter(config-dial-peer)#port 1/0:23
```

## ISDN-to-PBX and ISDN-to-PSTN Topology

Cisco.com

### Span Engineering West Coast Branch



### Typical Application Using BRI-NT/TE VICs or BVM4-NT/TE Voice Modules

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.21

A typical BRI deployment is shown in the figure. This is the procedure for configuring ISDN BRI for voice:

**Step 1** `isdn switch-type switch-type`

**Step 2** `interface bri number` or `interface bri slot/port`

---

**Note** Between Step 2 and Step 3, it is possible to set a switch type for the interface. This setting overrides the switch type set for the router.

---

**Step 3** `no ip address`

**Step 4** (optional) `isdn overlap-receiving`

**Step 5** (optional) `isdn twait-disable`

**Step 6** (optional, TE only) `isdn spid1 spid-number [ldn]`

**Step 7** (optional, TE only) `isdn spid2 spid-number [ldn]`

**Step 8** `isdn incoming-voice {voice | modem}`

**Step 9** `shutdown`

**Step 10** `isdn layer1-emulate {user | network}`

**Step 11** `no shutdown`

**Step 12** (optional, TE only) `network-clock-priority {low | high}`

**Step 13** `isdn protocol-emulate {user | network}`

**Step 14** `exit`

**Step 15** `clear interface bri number` or `clear interface bri slot/port`

**Step 16** Repeat for other interfaces

**Step 17** Configure dial peers. See the PRI example for dial-peer configuration.

An example procedure for configuring ISDN BRI for voice is shown in the “Configuring BRI Interfaces” table.

### Configuring BRI Interfaces

| Step | Action                                                                                                                                                 | Notes                                                                                                                                                                                                                                                                                                                               |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Router (config) # <b>isdn switch-type</b><br><i>switch-type</i>                                                                                        | Configure the global ISDN switch type to match the service-provider switch type.                                                                                                                                                                                                                                                    |
| 2.   | Enter interface configuration mode to configure parameters for the specified interface.<br>Router (config) # <b>interface bri</b><br><i>slot/port</i>  | <i>slot</i> is the location of the voice network module in the router.<br><i>port</i> is the location of the BRI VIC in the voice network module. Valid values are 0 or 1.<br><b>Note:</b> Between Steps 2 and 3, it is possible to set a switch type for the interface. This setting overrides the switch type set for the router. |
| 3.   | Specify that there is no IP address for this interface.<br>Router (config-if) # <b>no ip address</b>                                                   | For information about IP addressing, see the Cisco IOS software document <i>Network Protocols Configuration Guide, Part 1</i> .                                                                                                                                                                                                     |
| 4.   | Activate overlap signaling.<br>Router (config-if) # <b>isdn overlap-receiving</b>                                                                      | (Optional) In this mode, the interface waits for possible additional call-control information.                                                                                                                                                                                                                                      |
| 5.   | <b>twait</b> time is enabled by default.<br>Router (config-if) # <b>isdn twait-disable</b>                                                             | (Optional) Use this command when the ISDN switch type is basic-ni1. Delay a National ISDN BRI switch a random time before activating the Layer 2 interface when the switch starts up.                                                                                                                                               |
| 6.   | Specify a SPID and local directory number for the B1 channel.<br>Router (config-if) # <b>isdn spid1</b><br><i>spid-number [ldn]</i>                    | (Optional) Currently, only the DMS-100 and NI-1 switch types require SPIDs. Although the Lucent 5ESS switch type might support a SPID, you should set up that ISDN service without SPIDs.                                                                                                                                           |
| 7.   | Router (config-if) # <b>isdn spid2</b><br><i>spid-number [ldn]</i>                                                                                     | (Optional) Specify a SPID and local directory number for the B2 channel.                                                                                                                                                                                                                                                            |
| 8.   | Configure the port for incoming voice calls.<br>Router (config-if) # <b>isdn incoming-voice voice</b>                                                  | -                                                                                                                                                                                                                                                                                                                                   |
| 9.   | Configure the interface ISDN switch type to match the service-provider switch type.<br>Router (config-if) # <b>isdn switch-type</b> <i>switch-type</i> | (Optional) The interface ISDN switch type overrides the global ISDN switch type on the interface.                                                                                                                                                                                                                                   |
| 10.  | Turn off the port prior to setting the port emulation.<br>Router (config-if) # <b>shutdown</b>                                                         | -                                                                                                                                                                                                                                                                                                                                   |
| 11.  | Configure port mode emulation.<br>Router (config-if) # <b>isdn layer1-emulate</b> { <i>network</i> / <i>user</i> }                                     | <i>user</i> : Configures Layer 1 port mode emulation and clock status for the TE (clock slave)<br><i>network</i> : Configures Layer 1 port mode emulation and clock status for the NT (clock master)                                                                                                                                |
| 12.  | Turn on the port after setting port mode emulation.<br>Router (config-if) # <b>no shutdown</b>                                                         | -                                                                                                                                                                                                                                                                                                                                   |



| Step | Action                                                                                                                                                            | Notes                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 13.  | For TE only, set the priority for recovering clock signal from the network NT device for this BRI port.<br>Router (config-if) # <b>network-clock-priority low</b> | <b>high:</b> First priority and is default for BRI voice interface cards<br><b>low:</b> Low priority and is default for BRI voice modules |
| 14.  | Set Layer 2 and Layer 3 port-mode emulation<br>Router(config-if)# <b>isdn protocol-emulate {network   user}</b>                                                   | <i>user:</i> Sets port as TE (clock slave)<br><i>network:</i> Sets port as NT (clock master)                                              |
| 15.  | exit                                                                                                                                                              | -                                                                                                                                         |

## ISDN Connection to a PBX Configuration (Network-Side Emulation): Example

Cisco.com

- **Step #1 – Define the ISDN switch type**

```
SJ1Router(config)#isdn switch-type basic-ni
```

- **Step #2 – Enter interface configuration mode**

```
SJ1Router(config)#interface bri 1/0
```

- **Step #2 b – Define ISDN switch type for interface bri 1/0**

```
SJ1Router(config-if)#isdn switch-type basic-net3
SJ1Router(config-if)#exit
```

- **Step #3 and #4 – Set overlap signaling and twait or timers**

```
SJ1Router(config)#isdn overlap-receiving
SJ1Router(config)#isdn T306 10000
```

- **Step #5 to #7 – Not used in this example**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0 2-18

Once you have configured the BRI interfaces, the following is an excerpt of the output of a **show running-configuration** command configured for the router in San Jose 1:

```
isdn switch-type basic-ni
!
interface BRI1/0
 no ip address
 isdn switch-type basic-net3
!
isdn overlap-receiving
isdn t306 10000
isdn incoming-voice voice
isdn layer1-emulate network
isdn protocol-emulate network
!
```

---

**Note** Remember that the configuration of the switch type on the interface takes precedence over the switch type setting on the router.

---

## ISDN Connection to the PSTN Configuration (User-Side Emulation): Example

Cisco.com

- A running configuration sample from SF1Router

```
SF1Router#show running-config
interface BRI1/0
no ip address
isdn switch-type basic-ni1
isdn twait-disable
isdn spid1 14085552111 5552111
isdn spid2 14085552112 5552112
isdn incoming-voice voice
!
interface BRI1/1
no ip address
isdn switch-type basic-ni1
isdn twait-disable
isdn spid1 14085552111 5552111
isdn spid2 14085552112 5552112
isdn incoming-voice voice
```

© 2005 Cisco Systems, Inc. All rights reserved.

QWOK v1.0 2-20

Instead of stepping through the configuration for the user-side interface of the ISDN BRI example, the running configuration is shown in this figure. Observe the differences between this router from building San Francisco 1 and the one configured for San Jose 1. Specifically, you should note the following:

- The switch type does not have to be **basic-net3** or **basic-qsig** since it is not set up for network termination.
- The interface has not been specifically told that it is a user-side interface; it will default to a user-side interface.
- The **isdn twait-disable** command has been used because the switch type is **basic-ni1**.
- SPIDs have been defined because the switch type is **basic-ni1**.

# Troubleshooting ISDN Circuits

This topic describes the troubleshooting tools used to resolve ISDN issues.

## Common ISDN Issues

Cisco.com

- **System clocking**
- **Signaling mismatch**
- **Switch type mismatch**
- **Number type and plan mismatches**
- **Calling name display issues**
- **No ringback**
- **No busy tone**
- **ISDN timer issues**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0 2-21

## System Clocking

If timing between devices is not maintained, a condition known as clock slippage (or “clock slips”) might occur. By definition, a clock slip is the repetition or deletion of a bit (or block of bits) in a synchronous data stream due to a discrepancy in the read and write rates at a buffer. Slips arise because an equipment buffer store cannot accommodate differences between the phases or frequencies of the incoming and outgoing signals in cases where the timing of the outgoing signal is not derived from that of the incoming signal.

A T1 or E1 interface sends traffic inside repeating bit patterns that are called frames. Each frame is a fixed number of bits, which allows the device to determine the start and end of a frame. This also means that the receiving device knows exactly when to expect the end of a frame; it simply counts the appropriate number of bits that have come in. Therefore, if the timing between the sending and the receiving device is not the same, the receiving device might sample the bit stream at the wrong moment, which results in the return of an incorrect value.

While Cisco IOS software has the ability to easily control the clocking on these platforms, the default clocking mode on a time-division multiplexing (TDM)-capable router is effectively free running. This means that the received clock signal from an interface is not connected to the backplane of the router and is not used for internal synchronization between the rest of the router and its other interfaces. Therefore, the router uses an internal clock source to pass traffic across the backplane and across other interfaces.

For data applications, this generally does not present a problem because a packet is buffered in internal memory and is then copied to the transmit buffer of the destination interface. Packet reads and writes to memory effectively remove the need for any clock synchronization between ports.

Digital voice ports have a different issue. Unless otherwise configured, Cisco IOS software uses the backplane (or internal) clocking to control data reads and writes to the digital signal processors (DSPs). If a PCM stream comes in on a digital voice port, it uses the external clocking for the received bit stream. However, this bit stream does not necessarily use the same reference as the router backplane, which means that the DSPs might misinterpret the data that is coming in from the controller. This clocking mismatch is seen on the router E1 or T1 controller as a clock slip because the router is using its internal clock source to send the traffic out of the interface, but the traffic that is coming in to the interface is using a completely different clock reference. Eventually, the difference in the timing relationship between the transmit and the receive signals becomes so great that the interface controller registers a slip in the received frame.

The following Cisco IOS software platforms allow clocking to be propagated across the backplane of the router and between different interface ports: the Cisco AS5350 Universal Gateway, the Cisco AS5400 Series Universal gateways, the Cisco 7200VXR Router, the Cisco 2600 Series routers, the Cisco 3700 Series routers, and the Cisco 1760 Router. Depending on the installed hardware, all of the previously mentioned platforms use different command-line interface (CLI) commands to configure the clocking modes. Even though the syntax differs, they essentially tell the router to recover the clocking from a digital voice port and to use this signal to drive other router operations.

Since none of these commands are default, some network administrators do not initially see them in the router configuration files and, therefore, do not understand their significance.

In most cases, you can check for clock slips on the E1 or T1 interface to confirm the problem. Issue the **show controller {e1 | t1} command** for such confirmation. The following example output shows a periodic clock slip on the E1 interface:

```
Router# show controller e1 0/0
E1 0/0 is up.
 Applique type is Channelized E1 - balanced
 No alarms detected.
 alarm-trigger is not set
 Version info Firmware: 20020812, FPGA: 11
 Framing is CRC4, Line Code is HDB3, Clock Source is Line.
 Data in current interval (97 seconds elapsed):
 0 Line Code Violations, 0 Path Code Violations
 4 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded
 Mins
 4 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0
 Unavail Secs
```

## Signaling Mismatch

The most notable instance of switches being mismatched is the case where a PBX cannot be configured as terminal equipment and requires a network-side emulation to be configured on the voice gateway. If the PBX is connected to the gateway through a BRI TE interface, the connection does not work.

## Switch-Type Mismatch

ISDN is a standard, but switch manufacturers implement ISDN slightly differently. If switch types are mismatched, the passage of signaling information can be lost, which causes calls to fail. For instance, a PBX may require QSIG to send specific messages, but the PRIs connected to the voice gateway are not configured with QSIG. Switch-type keywords that can be used when configuring switch types with Cisco voice gateways are described in the “ISDN PRI and ISDN BRI Global Switch-Type Keywords” table.

## ISDN PRI and ISDN BRI Global Switch-Type Keywords

| Global Switch Type | Description                                                                      | PRI Interface  | BRI Interface |
|--------------------|----------------------------------------------------------------------------------|----------------|---------------|
| primary-4ess       | AT&T 4ESS switch type for the United States (ISDN PRI only)                      | primary-4ess   | basic-ni      |
| primary-5ess       | AT&T primary rate switches                                                       | primary-5ess   | basic-ni      |
| primary-dms100     | NT DMS100 switch type for the United States (ISDN PRI only)                      | primary-dms100 | basic-ni      |
| primary-net5       | Net5 ISDN PRI switches (Europe)                                                  | primary-net5   | basic-net3    |
| primary-ni         | -                                                                                | primary-ni     | basic-ni      |
| primary-ntt        | Intelligent Network Server (INS) Net1500 for Japan (ISDN PRI only)               | primary-ntt    | basic-ntt     |
| primary-qsig       | -                                                                                | primary-qsig   | basic-qsig    |
| primary-ts014      | Australian TS014 switches (ISDN PRI only)                                        | primary-ts014  | basic-ts013   |
| basic-1tr6         | German 1TR6 ISDN switches                                                        | primary-net5   | basic-1tr6    |
| basic-5ess         | AT&T basic-rate switches                                                         | primary-ni     | basic-5ess    |
| basic-dms100       | NT DMS100 basic rate switches                                                    | primary-ni     | basic-dms100  |
| basic-net3         | Net3 ISDN and European ISDN switches (UK and others), also called E-DSS1 or DSS1 | primary-net5   | basic-net3    |
| basic-ni           | National ISDN-1 switches                                                         | primary-ni     | basic-ni      |
| basic-ntt          | Japanese NTT ISDN switches (ISDN BRI only)                                       | primary-ntt    | basic-ntt     |
| basic-qsig         | -                                                                                | primary-qsig   | basic-qsig    |
| basic-ts013        | Australian TS013 switches                                                        | primary-ts014  | basic-ts013   |
| basic-vn3          | VN3 French ISDN switches (ISDN BRI only)                                         | primary-net5   | basic-vn3     |

### Numbering Type and Plan Mismatches

If the proper digits are being sent to the PSTN, but the call is not being routed properly, check to make sure that the numbering plan and type are set in accordance with the way the device connected to the gateway is configured.

By default, for calls to route patterns containing the NANP “@” wildcard, the called party numbering type is classified as national (international if 011 is dialed), and the called numbering plan is ISDN. For calls to route patterns not containing the NANP @ wildcard, the called party numbering plan and type are classified as “unknown”. The calling party numbering plan and type can be classified differently, depending on the digits to be sent.

If there is a suspected problem with the numbering plan or type, try changing the calling and called party numbering plan to national and the numbering type to ISDN. If the country you are in has a different numbering type, experiment with different values to resolve the issue.

Whatever the case, make sure that the called and calling party are being classified correctly so that the CO can process that call. If you are unsure what the plan and type should be set to, contact your service provider and ask.

---

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | If a PRI or a BRI is configured with overlap sending, dialed digits will be sent one at a time and can make the system sensitive to dial-peer errors. For instance, if dial peer 3 is VoIP and has destination pattern 408..... and dial peer 1 is plain old telephone service (POTS) and has destination pattern 4085550123, dial peer 3 will be triggered as soon as the gateway registers the 408. If the default en-bloc signaling is on for ISDN, the gateway waits until all the digits have arrived before matching to a dial peer. |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## Calling Name Display Problems

A common problem network administrators encounter between a voice gateway and a PBX is the ability to pass calling-name information. The display IE is commonly used to pass calling-name information over PRI. However many PBXs, in addition to some service provider NI3-type ISDN switches, only support the passage of calling name information with the facility IE in QSIG. If this is suspected as an issue, contact the PBX vendor for details.

Some service providers provide calling-name display service from the PSTN on ISDN PRIs configured for the NI3 switch type. NI3 also uses a facility IE to send calling name information. The N12 switch type is only supported on the Cisco CallManager version 3.3 and later. Therefore, Cisco CallManager cannot accept calling-party name information from a service provider that sends the name in a facility IE, but it supports any device sending the name in a Display IE.

Cisco CallManager provides calling-name display if the “Display IE Delivery” checkbox is checked on the receiving gateway (either H.323 or MGCP). Either Cisco CallManager traces calling name information that has been sent or received or **debug isdn q931** output from a Cisco IOS gateway shows it to you. If you see the name being presented to the far end and it is not showing up, you need to work with the administrators of that equipment to determine why they are not accepting the name information.

As a general rule, Lucent or Avaya PBX equipment can send and receive calling name information using most switch types as long as it is configured to send the display information in code set 0 (this is a trunk group configuration parameter on the PBX).

Message types that are used to send specific caller identification information are shown for PRI trunks and QSIG trunks in the “Signaling of Caller Identification Information by Device Control Protocols” table.

### Signaling of Caller Identification Information by Device Control Protocols

| Device Control Protocol | Calling Line               | Calling Name                              | Connected Line            | Connected Name                            |
|-------------------------|----------------------------|-------------------------------------------|---------------------------|-------------------------------------------|
| PRI trunk               | calling line in PRI SETUP  | supported by FACILITY IE in PRI messages  | not supported             | supported by FACILITY IE in PRI messages  |
| QSIG trunk              | calling line in QSIG SETUP | supported by FACILITY IE in QSIG messages | supported by QSIG CONNECT | supported by FACILITY IE in QSIG messages |

## No Ringback

The following situations can occur where there is no ringback on VoIP calls or on calls between IP and POTS phones:

- No ringback tone on VoIP toll-bypass calls:
  - Symptom: POTS (PSTN/PBX) user places a call (through Cisco router or gateways) and does not hear a ringback tone before the call is answered.
  - Solution 1: Configure the Cisco IOS global configuration command **voice call send-alert** in the terminating gateway or router. This command enables the terminating gateway to send an alert message instead of a progress message after it receives a call setup.
  - Solution 2: If the previous solution does not work, configure the terminating gateway to send a progress indicator (PI) = 8 in the alert message by configuring the **progress\_ind alert enable 8** command under the POTS dial-peer configuration. This command overrides the PI value received in the ISDN alert message and causes the router to cut through the audio path back toward the calling party prior to connecting.

---

**Note** The **progress\_ind alert** and the **progress\_ind setup** commands are hidden in some versions of Cisco IOS software and may not be visible within the help parser. However, if the **progress\_ind progress** command is available in the help parser, the above commands are also available and can be entered into the dial peer in their entirety. These commands will subsequently appear in the running configuration.

---

- No ringback tone on VoIP inbound calls to Cisco CallManager (or third-party VoIP devices) through Cisco IOS gateway:
  - Symptom: POTS (PSTN/PBX) user places a call to an IP phone (through a Cisco router or gateway) and does not hear a ringback tone before the call is answered.
  - Solution: Configure the Cisco IOS command **progress\_ind setup enable 3** under the VoIP dial-peer configuration in the Cisco gateway or router. This command forces the gateway or router to treat the inbound ISDN setup message as if it came in with a PI = 3 and to generate an in-band ringback tone toward the calling party if the H.225 alert message does not contain a PI of 1, 2, or 8.
- No ringback tone on VoIP outbound calls from Cisco CallManager (or third-party VoIP devices) through Cisco IOS gateway:
  - Symptom: User places a call from IP phone or third-party device to an outside number through a Cisco router or gateway and does not hear a ringback tone.
  - Solution 1: Ringback tones must come from the PSTN for trunk circuits in this situation. There are two dial-peer subcommands that may help. On the IOS router or gateway use the **progress\_ind alert enable 8** command under the outgoing POTS dial-peer configuration. This command presents the Q.931 alert message to the software on the router or gateway as if the alert message had a PI of 8 and cut through the audio path.



- Solution 2: If the previous command does not solve the problem, use the (Cisco IOS Software Release 12.2(1) or 12.2(2)T and later) **progress\_ind setup enable 3** command under the POTS dial-peer configuration. This command causes the gateway to send a PI with a value of 3 in the ISDN setup message, which indicates to the PSTN or a PBX that the originating device is not an ISDN device and in-band information should be presented. This command should be used in conjunction with the **progress\_ind alert enable 8** command.
- Solution appendix: If the PSTN device is not able to generate ringback in-band (for example, an ISDN phone directly connected to a BRI port on the gateway), the gateway can be configured to generate ringback on the IP call leg by using the **tone ringback alert-no-pi** command on the POTS dial peer. When the ISDN alert is received with no PI present, the gateway generates the ringback and includes a PI = 0x8 in the H.225 alert message.
- No ringback tone when call is transferred from Cisco CallManager or Unity voice mail:
  - Symptom: An incoming call from a Cisco gateway or router to Cisco CallManager or Unity voice mail that is transferred after the call is answered does not hear ringback.
  - Solution: To solve this problem you can either follow the steps outlined below, or you can configure the Cisco IOS gateway or router as an MGCP gateway instead of as an H.323 gateway: To attempt to solve the problem for H.323, you must first have Cisco CallManager 3.0(8) or later. From the Cisco CallManager Administration page, go to the Service menu and select **Service Parameters**. For each active Cisco CallManager server, perform the following steps:
    - Step 1** In the Configured Services box, select **Cisco CallManager**.
    - Step 2** In the Param drop-down list box, select **ToSendH225UserInfoMsg**.
    - Step 3** Set the Value drop-down list box to **T** for true.
    - Step 4** Upgrade the router or gateway Cisco IOS software to version 12.2(2.4) or higher.

### No Busy Tone on Outbound VoIP Calls

Symptom: A Cisco IP phone (Cisco CallManager scenario) or POTS phone (VoIP toll-bypass scenario) does not hear a busy tone or announcement message from the PSTN network.

Solution: Use the Cisco IOS software **voice call convert-discp-i-to-prog** global configuration command (Cisco IOS Software Release 12.2(1) and later). This command converts an inbound ISDN disconnect message with a PI to an H.225 progress message with the same PI value. This command can help when an announcement is played on the terminating PSTN side, but the calling party does not hear the response.

### ISDN Timer Issues

The ISDN Q.931 specification lists a variety of timers that dictate how long an ISDN device should wait for a certain event to occur before taking corrective action. The Q.921 specification also lists a variety of timers related to D-channel establishment procedures. However, adjusting these timers is seldom required.

Understanding how these timers work and when they are used is important especially if you are troubleshooting calls that are being disconnected with a cause code of 0xE6, “Recovery on timer expiry.” This cause code indicates that the call was disconnected because a timer expired and there was no further corrective action that could be taken other than disconnecting the call.

The cause code in the cause IE is sometimes followed by the name of the timer that has expired (for example, 03 01 00—the 310 timer).

For example, if a voice gateway sends a call out to the PSTN by sending a SETUP message and the voice gateway receives a CALL PROCEEDING from the PSTN as expected, the T310 timer starts. This timer specifies that the gateway must receive either ALERTING, CONNECT, or DISCONNECT from the PSTN before the timer expires. By default, this timer is 10 seconds. After 10 seconds, the Cisco CallManager sends a DISCONNECT with a cause of “Recovery on Timer Expiry.”

## Common ISDN Debug Commands

Cisco.com

| Command                                        | Purpose                                                                                                                                    |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show controllers<br/>bri number</b> | Checks Layer 1                                                                                                                             |
| Router# <b>show isdn status</b>                | Validates Layer 1 and Layer 2. Follow up with <b>debug q931</b>                                                                            |
| Router# <b>debug isdn<br/>events</b>           | Display ISDN events occurring on the user side of the ISDN interface                                                                       |
| Router# <b>debug q921</b>                      | Display Layer 2 access procedures that are taking place at the router on the D channel                                                     |
| Router# <b>debug q931</b>                      | display information about call setup and teardown of Layer 3 ISDN network connections between the local router (user side) and the network |

© 2005 Cisco Systems, Inc. All rights reserved.

QWOK v1.8 2-22

The “Common ISDN Issues” figure showed issues common to ISDN call disconnects or failure. This figure shows some of the commands that are commonly used in a systematic procedure to troubleshoot ISDN circuits. PRI troubleshooting begins with the techniques that are standard with T1 and E1 circuits. Follow this sequence:

**Step 1** Confirm that the controller is active and that there are no alarms. If there is a red alarm, your equipment attempts to send a yellow alarm to the remote end to notify the user that you are experiencing a problem.

---

**Note** A red alarm is for a loss of frame (LOF) or loss of signal (LOS) and means that the proper information is not being received from the service provider network.

---

**Step 2** After verifying that there are no alarms, check the controller for path code violations and clock slips.

**Step 3** If there continues to be a problem, check the ISDN network status with the **show isdn status** command. This command is described later in this section.

**Step 4** If Layer 1 and Layer 2 are verified with the **show isdn status** command and the problem persists, use the **debug isdn q931** command (shown in the “Common ISDN Debug Commands” figure) to monitor the direction of the disconnect, then confirm that the bearer capability is correct. For example, a voice call may be coming in as data. A disconnect cause code of “Bearer Capability not Implemented” typically means that a command such as **isdn incoming-voice modem** is missing from the D-channel configuration.

**Step 5** At this stage, if calls are still failing, determine the status of the attempted channel with the **show isdn status** command. If the call is being attempted on the B channel, for some reason it has busied out. The B channel can be manually reset.

**Step 6** Finally, if there is still no resolution, the **debug q931** command tells you what the cause code is, although it does not necessarily spell out the problem for you since cause codes have a tendency to be rather cryptic.

## Common ISDN Debug Commands

Cisco.com

| Command                                    | Purpose                                                                                                                                    |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show controllers bri number</b> | Checks Layer 1                                                                                                                             |
| Router# <b>show isdn status</b>            | Validates Layer 1 and Layer 2. Follow up with <b>debug q931</b>                                                                            |
| Router# <b>debug isdn events</b>           | Display ISDN events occurring on the user side of the ISDN interface                                                                       |
| Router# <b>debug q921</b>                  | Display Layer 2 access procedures that are taking place at the router on the D channel                                                     |
| Router# <b>debug q931</b>                  | display information about call setup and teardown of Layer 3 ISDN network connections between the local router (user side) and the network |

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0 2-22

The five commands presented in this figure and the previous figure are the five commands that are most commonly used to troubleshoot problems with ISDN.

The **show isdn status** command is used to verify that the ISDN BRI Layer 1 is ACTIVE, the Layer 2 state is MULTIPLE\_FRAME\_ESTABLISHED, and the SPIDs are valid. If all of these conditions are satisfied, the problem is probably not with ISDN Layer 1 or Layer 2, and troubleshooting should focus on ISDN BRI Layer 3 using the **debug isdn q931** command. If a TEI\_UNASSIGNED or AWAITING\_ESTABLISHMENT state is reported, verify the configuration. Remember that for a back-to-back configuration, such as in a connection between a voice gateway and a PBX, one of the sides must be set to emulate the network.

---

**Note** Remember, if network emulation is not set, Layer 2 will not come up.

---

When the **show isdn status** command is used, watch for the following types of output concerning the voice network:

- Layer 1 Status: DEACTIVATED. This message means that the router is not establishing a Layer 1 connection to the service provider ISDN switch. Follow these steps:
  - Use the **shutdown**, then the **no shutdown** command on the BRI interface in question. This action ensures that the BRI interface is not administratively down. You can also perform a **clear interface bri number** to reset the interface.
  - Verify that the **backup interface** command is not configured under the BRI interface. This command deactivates the BRI interface until the backup is initiated. If necessary, use the **no backup interface interface\_type interface\_number** command to remove it.
  - Use the **show isdn status** command to check if the switch type for the interface is correctly configured. If the switch type is not configured or is configured incorrectly, configure it on the interface.

■ Layer 2 Status: Layer 2 NOT Activated

- Layer 2 problems often cannot be rectified at the customer site. However, Layer 2 debugs (or the interpretation of the debugs) can be provided to the service provider for their reference. The **debug isdn q921** command output provides details on the Layer 2 transaction occurring between the ISDN switch and the router.
- Pay attention to the direction of the messages. The debugs indicate if the messages were generated by the router (indicated by TX ->) or if they were received by the router (indicated by RX <-). In the example below, the first message (IDREQ) is sent by the router, while the second (IDASSN) is from the ISDN switch:

```
*Mar 1 00:03:46.976: ISDN BR0: TX -> IDREQ RI = 29609 AI = 127
*Mar 1 00:03:47.000: ISDN BR0: RX <- IDASSN RI = 29609 AI = 96
```

- You can identify the source of the problem by following the direction of a particular message and the response. For example, if the telephone company ISDN switch unexpectedly sends a Layer 2 disconnect, the router will reset Layer 2 also. This event indicates that the problem lies with the telephone company ISDN switch.

■ SPID Status: SPID number NOT valid

■ Layers 1 and 2 are Active; SPIDs are Valid

All debug commands are entered in privileged EXEC mode, and most debug commands take no arguments. For example, to enable the **debug isdn q931** command, enter the command in privileged EXEC mode.

To turn off the **debug isdn q931** command, in privileged EXEC mode, enter the **no** form of the command at the command line.

Alternately, in privileged EXEC mode, you can enter the **undebug isdn q931** form of the command.

To display the state of each debugging option, enter the **show debugging** command in privileged EXEC mode at the command line.

---

**Note** Normally, the router generates debugging messages for every interface, resulting in a large number of messages that consume system resources and make it difficult to find the specific information you need. By limiting the number of debugging messages, you can receive messages related to only the ports you want to troubleshoot.

---

The **show isdn status** command is very useful when you are troubleshooting ISDN signaling problems. This command displays a summary of the status of all ISDN interfaces, and it displays the status of Layers 1, 2, and 3. The following is an example of **show isdn status** command output:

```
WDGRouter#show isdn status
Global ISDN Switchtype = primary-5ess
ISDN Serial0:23 interface
 dsl 0, interface ISDN Switchtype = primary-5ess
 Layer 1 Status:
 ACTIVE
 Layer 2 Status:
 TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
 Layer 3 Status:
 5 Active Layer 3 Call(s)
 Activated dsl 0 CCBs = 5
```

```
CCB:callid=7D5, sapi=0, ces=0, B-chan=9, calltype=DATA
CCB:callid=7D6, sapi=0, ces=0, B-chan=10, calltype=DATA
CCB:callid=7DA, sapi=0, ces=0, B-chan=11, calltype=DATA
CCB:callid=7DE, sapi=0, ces=0, B-chan=1, calltype=DATA
CCB:callid=7DF, sapi=0, ces=0, B-chan=2, calltype=DATA
The Free Channel Mask: 0x807FF8FC
ISDN Serial1:23 interface
 dsl 1, interface ISDN Switchtype = primary-5ess
Layer 1 Status:
 ACTIVE
Layer 2 Status:
 TEI = 0, Ces = 1, SAPI = 0, State = TEI_ASSIGNED
Layer 3 Status:
 0 Active Layer 3 Call(s)
Activated dsl 1 CCBS = 0
The Free Channel Mask: 0x807FFFFFF
Total Allocated ISDN CCBS = 5
```

## Troubleshooting ISDN Incoming Calls

Cisco.com

```
Router# debug isdn q931
RX <- SETUP pd = 8 callref = 0x06
 Bearer Capability i = 0x8890
 Channel ID i = 0x89
 Calling Party Number i = 0x0083, \Q5551234`
TX -> CONNECT pd = 8 callref = 0x86
RX <- CONNECT_ACK pd = 8 callref = 0x06
```

- **An example of a successful connection**

© 2005 Cisco Systems, Inc. All rights reserved.

©WOK v1.0 2-23

Use the **debug isdn q931** command to watch the Q931 signaling messages go back and forth while the router negotiates the ISDN connection. The figure shows the output of a successful connection.

The SETUP message indicates that the connection is initiated by the remote end. The call reference numbers are maintained as a pair. In this case, the call reference number for the incoming side of the connection is 0x06, while the call reference number of the outbound side of the connection is 0x86. The bearer capability (often referred to as the “bearercap”) tells the router what kind of call is coming in. In this case, the connection is type 0x8890, which indicates “ISDN speed 64 kbps.” If the bearercap had been 0x8090A2, it would have indicated “Speech/voice call u-law.”

If you do not see a SETUP message, verify the correct number (if the number is voice-provisioned, try calling it manually) and check the status of the ISDN interface.

If the number is correct and the ISDN interface is working, make sure that the call originator is making the correct call. Contact the telephone company to trace the call to see where it is being sent. If the connection is a long-distance one, try a different long-distance carrier using a 1010 long-distance code.

If the call coming in is an asynchronous modem call, make sure that the line is provisioned to allow voice calls.

---

**Note** BRI asynchronous modem calling is a feature of Cisco 3600 Series routers running Cisco IOS Software Release 12.0(3)T or later. The asynchronous modem calling feature requires a recent hardware revision of the BRI interface network module. WAN interface card (WIC) modules do not support asynchronous modem calling.

---

If the call arrived but did not complete, look for a cause code. The “ISDN Cause Value” table provides a translation of the cause codes that may be presented.

## ISDN Cause Value

| Hex Value | Cause                                   | Explanation                                                                                                                                                                                                                               |
|-----------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 81        | Unallocated (unassigned) number         | The ISDN number was sent to the switch in the correct format; however, the number is not assigned to any destination equipment.                                                                                                           |
| 90        | Normal call clearing                    | Normal call clearing has occurred.                                                                                                                                                                                                        |
| 91        | User busy                               | The called system acknowledges the connection request but is incapable of accepting the call because all B channels are in use.                                                                                                           |
| 92        | No user responding                      | The connection cannot be completed because the destination does not respond to the call.                                                                                                                                                  |
| 93        | No answer from user (user alerted)      | The destination responds to the connection request but fails to complete the connection within the prescribed time. The problem is at the remote end of the connection.                                                                   |
| 95        | Call rejected                           | The destination is capable of accepting the call, but it rejected the call for an unknown reason.                                                                                                                                         |
| 9C        | Invalid number format                   | The connection could not be established because the destination address was presented in an unrecognizable format or because the destination address was incomplete.                                                                      |
| 9F        | Normal, unspecified                     | This reports the occurrence of a normal event when no standard cause applies. No action is required.                                                                                                                                      |
| A2        | No circuit/channel available            | The connection cannot be established because no appropriate channel is available to take the call.                                                                                                                                        |
| A6        | Network out of order                    | The destination cannot be reached because the network is not functioning correctly, and the condition might last for an extended period. An immediate reconnect attempt will probably be unsuccessful.                                    |
| AC        | Requested circuit/channel not available | The remote equipment cannot provide the requested channel for an unknown reason. This might be a temporary problem.                                                                                                                       |
| B2        | Requested facility not subscribed       | The remote equipment supports the requested supplementary service by subscription only. This is frequently a reference to long-distance service.                                                                                          |
| B9        | Bearer capability not authorized        | The user requested a bearer capability that the network provides, but the user is not authorized to use it. This might be a subscription problem.                                                                                         |
| D8        | Incompatible destination                | This indicates that an attempt was made to connect to non-ISDN equipment, for example, to an analog line.                                                                                                                                 |
| E0        | Mandatory information element missing   | The receiving equipment received a message that did not include one of the mandatory information elements. This is usually the result of a D-channel error. If this error occurs systematically, report it to your ISDN service provider. |
| E4        | Invalid information element contents    | The remote equipment received a message that includes invalid information in the information element. This is usually the result of a D-channel error.                                                                                    |



A successful completion is shown by a CONNECT-ACK message.

At this point, the ISDN call is connected, but no data has been seen coming across the link. Use the **debug ppp negotiate** command to see whether any Point-to-Point Protocol (PPP) traffic is coming across the line. If not, there may be a speed mismatch. To determine whether this is the case, use the **show running-config** privileged EXEC command to view the router configuration.

---

**Note** By default, ISDN interfaces attempt to use 64-kbps communication speeds on each channel.

---

## Troubleshooting ISDN Outbound Calling

Cisco.com

```
*Mar 20 21:07:45.025: ISDN BR0: Event: Call to 5553759 at 64 Kb/s
*Mar 20 21:07:45.033: ISDN BR0: TX -> SETUP pd = 8 callref = 0x2C
*Mar 20 21:07:45.037: Bearer Capability i = 0x8890
*Mar 20 21:07:45.041: Channel ID i = 0x83
*Mar 20 21:07:45.041: Keypad Facility i = 0x353533373539
*Mar 20 21:07:45.141: ISDN BR0: RX <- CALL_PROC pd = 8 callref = 0xAC
*Mar 20 21:07:45.145: Channel ID i = 0x89
*Mar 20 21:07:45.157: ISDN BR0: received HOST_PROCEEDING
 Channel ID i = 0x0101
*Mar 20 21:07:45.161: -----
 Channel ID i = 0x89
*Mar 20 21:07:45.313: ISDN BR0: RX <- CONNECT pd = 8 callref = 0xAC
*Mar 20 21:07:45.325: ISDN BR0: received HOST_CONNECT
```

- An example of a normal successful call

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0 2-24

Debugging outbound calls is very similar to debugging incoming calls. For outbound ISDN calls, **debug isdn q931** and **debug isdn events** commands are the best tools to use. The screen capture shows what a normal successful call might look like.

The first thing to check at the first suspicion of an ISDN failure, on either a BRI or a PRI, is the output from **show isdn status** command. The key things to note are that Layer 1 should be active and Layer 2 should be in a state of `MULTIPLE_FRAME_ESTABLISHED`.

The `CONNECT` message is the key indicator of success. If a `CONNECT` is not received, you may see a `DISCONNECT` or a `RELEASE_COMP` (release complete) message followed by a cause code. The following example provides the output of this type of message:

```
*Mar 20 22:11:03.212: ISDN BR0: RX <- RELEASE_COMP pd = 8 callref = 0x8F
*Mar 20 22:11:03.216: Cause i = 0x8295 - Call rejected
```

If you see the line “Cause i = 0x8090 - Normal call clearing”, the likely reason for a disconnection is a higher-protocol failure.

The cause value indicates two things. The second byte of the 4- or 6-byte value indicates from where in the end-to-end call path the `DISCONNECT` or `RELEASE_COMP` was received. This can help you to localize the problem. The third and fourth bytes indicate the actual reason for the failure.

## Troubleshoot MGCP PRI Backhaul Channels

Cisco.com

```
Router#show ccm-manager backhaul
PRI Backhaul Link info:
 Link Protocol: TCP
 Remote Port Number: 2428
 Remote IP Address: 172.18.106.59
 Current Link State: OPEN
 Statistics:
 Packets recvd: 2068
 Recv failures: 0
 Packets xmitted: 1521
 Xmit failures: 0
 PRI Ports being backhauled:
 Slot 1, port 1
```

- **Output from show ccm-manager backhaul command**

© 2005 Cisco Systems, Inc. All rights reserved.

QWOK v1.0 2-25

The one thing that distinguishes a PRI from other interfaces is the fact that the data that is received from the PSTN on the D channel needs to be carried in its raw form back to the Cisco CallManager for processing. An MGCP gateway does not process or modify this information. To do this, Cisco IOS MGCP gateways use a protocol called PRI backhaul.

The way PRI backhaul works is that everything up to the Layer 2 information, including all the Q.921 signaling, terminates on the gateway. This process means that the gateway takes care of D-channel establishment, but only under the direction of the Cisco CallManager. The gateway does not bring up the D channel unless it can communicate with the Cisco CallManager to backhaul the Q.931 messages contained in the D channel.

The screen capture shows the status of the backhaul channel. Use the **show ccm-manager backhaul** command to display this output.

---

**Note** This output is also included as part of the generic **show ccm-manager** command.

---

## Troubleshoot MGCP PRI Backhaul Channels (Cont.)

Cisco.com

```
Out Message -- PriSetupMsg -- Protocol= PriNi2Protocol
Ie - Ni2BearerCapabilityIe IEData= 04 03 80 90 A2
Ie - Q931ChannelIdIe IEData= 18 03 A9 83 97
Ie - Q931CallingPartyIe IEData= 6C 06 00 80 32 30 30 30
Ie - Q931CalledPartyIe IEData= 70 05 80 32 30 30 31
MMan_Id= 0. (iep= 0 dsl= 0 sapi= 0 ces= 0 IpAddr=61e100a IpPort=2427)
IsdnMsgData2= 08 02 00 02 05 04 03 80 90 A2 18 03 A9 83 97 6C
06 00 80 32 30 30 30 70 05 80 32 30 30 31
```

- **Output from ISDN Trace Message from a CCM Trace File**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0 2-28

ISDN traces assist with troubleshooting PRI trunks. An ISDN trace can determine what calling numbers and called numbers are involved in a call and the reason for a call termination. The reason is provided in the cause code in the disconnect message.

---

**Note** The easiest way to read ISDN traces is with the Q.931 translator. In this lesson, a raw trace file will be used.

---

The critical data in the setup message shown in the figure is highlighted. This is an outbound setup message toward the PSTN. The digits for calling and called party numbers are encoded in ASCII. Since the digits 0 to 9 are represented by ASCII characters 30 to 39, removing the leading 3 from each byte gives you the digit. For example, the trace shows 32 30 30 30 in the Q931CallingPartyIe field. If you ignore the 3s, you can see that the calling party is 2000. Similarly, you can see that the called party is 2001 by looking at the Q931CalledPartyIe, which shows 32 30 30 31.

The IP address of this gateway is shown in hexadecimal notation as 61e100a. The number is disassembled two digits at a time starting from the right. Translated into decimal, the hexadecimal digits are as follows:

```
0x0a = 10
0x10 = 16
0x1e = 30
0x6 = 6
```

The IP address of this gateway is 10.16.30.6.

Also, this call is being sent out on channel 23 of the PRI. You can determine this by decoding the channel ID IE using the Q.931 specification. In this case, look at the last octet of the channel ID IE—in this case, 0x97. You must remove the most significant bit. Since 0x9 is 1001 in binary when you remove the most significant bit, you are left with 0001, which is 0x1. Similarly, if the value begins with 0x8, which is 1000 in binary, the removal of the most significant bit reduces it to 0000 in binary, which is 0x0 in hex. In this example, start with the last octet of the channel ID IE, which was 0x97. After converting the 0x9 part of the number to 0x1 by removing the most significant bit, you are left with 0x17. Converting 0x17 to decimal gives you 23. Because a PRI has only 23 B channels, the value of the channel ID IE is between 0x80 (channel 0) and 0x97 (channel 23).

Finally, the IsdnMsgData2 line contains a hexadecimal dump of the entire Q.931 packet. If you look at the IsdnMsgData2 line, it always begins with 08 for most signaling messages. The exception is link-management messages such as service messages that use 03. The following byte represents the length of the call reference and is either 01 or 02. You usually see a 2-byte call reference. Depending on the length, the next one or two bytes are important. These bytes are set to 00 02. This is the call reference value, and the most significant bit toggles depending on the message direction. A recommended practice is that you copy the last three digits and search through the file for that. In this case, you would search for 0 0F.

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- ISDN service is provided as 192-kbps “2B+D” BRI trunks or 1.544Mbps “23B+D” T1 PRI trunks or 2.048-Mbps “30B+D” E1 PRI trunks
- Some PBXs are unable to behave as terminal equipment and will only communicate to the voice gateway when a BRI network side interface is configured on the gateway
- The layer 3 Q.931 frame contains messages such as ALERTING, SETUP, and CONNECT. These messages are supported in carrying out their function by Information Elements such as FACILITY, DISPLAY, PROGRESS, and CAUSE
- Facility and Display IEs ensure that the PSTN gets the correct numbering plan information so that calls will be completed
- Common issues with ISDN circuits include system clocking, signaling mismatch, switch mismatch, numbering plan, and ISDN timer
- Care must be taken to ensure that PBX requirements for network and user side are met for trunk configuration with any of the Cisco voice gateways
- Cisco CallManager Trace messages, the Q.931 translator, and Cause information elements are the diagnostic tools that can help system administrators isolate BRI or PRI problems in their networks

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0 2-27

## 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) Explain what the network side of an ISDN connection does. (Source: Network Side vs. User Side)

---

---

---

- Q2) A SIP voice gateway running Cisco IOS Software Release 12.3(13) is connected to the PSTN with a PRI. Calls between the voice gateway and the PSTN work perfectly except that there is no ringback when dialing from the PSTN to the voice gateway because the voice gateway does not pick up and establish the call until it negotiates an RTP stream. That negotiation does not occur until after the call is picked up, which may be 30 to 60 seconds or until it is forwarded to voice mail. Once either event happens, the RTP stream is established and the call begins. How can the voice gateway generate ring back before the called party answers the call? (Choose two.) (Source: Common ISDN Implementation Requirements)

- A) Configure the dial peer with the following command:  
dial-peer voice # pots  
    progress\_ind setup enable 3  
    progress\_ind progress enable 8
- B) Configure the dial peer with the following command:  
dial-peer voice # voip  
    progress\_ind setup enable 3
- C) Tones being sent in the RTP bearer stream with cisco-rtp will not be sent because the RTP stream is not being negotiated until the call is being answered. The network should be switched over to an out-of-band-type tone relay.
- D) Reconfigure the voice gateway as MGCP instead of SIP and try again.
- E) This situation cannot occur. During setup, the setup acknowledge message will send back a PI = 8, which sets the endpoint for early alert.

- Q3) Write the command sequence that will set the switch type for a gateway to **primary-ni**. (Source: Common ISDN Implementation Requirements)

---

- Q4) Which of the following best describes a clock slip? (Source: Troubleshooting ISDN Circuits)
- A) A clock slip is when ISDN timers clear calls early based on an unexpected PI in the signaling stream.
  - B) A clock slip is when the two ends of a connection are using different timing sources that keep time slightly differently causing one end to register an incorrect bit pattern.
  - C) A clock slip is when the network side and the PSTN cannot agree on a clock standard, and the network side clock is allowed to slip in order to synchronize it with the PSTN clock.
  - D) A clock slip is the amount of time that is lost between a PBX and a voice gateway in a certain period.



## Lesson Self-Check Answer Key

- Q1) ISDN requires a master-to-slave relationship on trunks to resolve conflicts that might exist when two endpoints in a call request the same thing but only one of the two can gain access to the resource at a time.
- Q2) B, D
- Q3) Router(config)#**isdn switch-type primary-ni**
- Q4) B



## Lesson 5

---

# QSIG Integration

---

### Overview

Frequently referred to as an inter-private branch exchange (inter-PBX) signaling system, Q Signaling (QSIG) is a protocol based on ISDN that enables signaling between nodes. QSIG is widely deployed to provide interoperability between different voice communications platforms in a multivendor environment. QSIG supports many supplementary services between PBXs. For Cisco platforms, a few key services have been singled out for support by Cisco voice gateways or by Cisco CallManager.

There are few Cisco IOS commands for QSIG that are separate from those used with ISDN. Therefore, it is important to know that QSIG is different from standard ISDN; QSIG is more complex.

This lesson describes how to integrate a voice gateway to the public switched telephone network (PSTN) or a PBX using QSIG.

### Objectives

Upon completing this lesson, you will be able to integrate a voice gateway into the PSTN or a PBX using QSIG. This ability includes being able to meet these objectives:

- Describe QSIG technology and why it is deployed in a voice gateway
- Describe QSIG network and user side switch types
- Describe common QSIG issues when deploying a gateway
- Configure a gateway to support QSIG connections
- Describe the troubleshooting tools that are used to resolve QSIG issues

# QSIG Circuit Overview

This topic describes QSIG technology and why QSIG would be deployed in a voice gateway.

## QSIG Circuit Overview

Cisco.com

### QSIG Facts

- **A variant of ISDN**
- **Enables PBX feature transparency across the WAN**
- **Eliminates multiple tandem PBX hops to reach a desired destination**
- **Becoming the standard for PBX interoperability in Europe and North America**

| OSI Layer       | Original ISDN                 | Q.SIG ISDN                                                 |
|-----------------|-------------------------------|------------------------------------------------------------|
| <b>7 to 4</b>   | <b>Application Mechanisms</b> |                                                            |
| <b>Network</b>  | Q.931                         | <b>QSIG-SS</b><br><b>QSIG-GF (Q.932)</b><br><b>QSIG-BC</b> |
| <b>Link</b>     | LAP-D                         | LAP-D                                                      |
| <b>Physical</b> | I.430<br>I.431                | I.430<br>I.431                                             |

© 2005 Cisco Systems, Inc. All rights reserved.
GWGK v1.0-2.3

QSIG is the informal name for the Private Signaling System Number 1 (PSS1) protocol. It was originally specified by the European Computer Manufacturers Association (ECMA) and then adopted by the European Telecommunications Standards Institute (ETSI) and the International Organization for Standardization (ISO). QSIG ensures that the essential functions in Q.931 are carried from node to node in private integrated services networks (PISNs) that have equipment from several vendors. QSIG is becoming the standard for PBX interoperability in Europe and North America. QSIG functions with the following three sub-layers:

- QSIG basic call (BC) extends Q.931 for use in a PISN and provides support for call setup, clearing, information, and maintenance. QSIG BC conforms to European Telecommunications Standards Institute (ETSI) codes 300, 171, and 172.
- QSIG generic function (GF) enables the transparent passage of facility and notify messages for the control of supplementary services and additional network features over a PISN.
- QSIG supplementary services provide additional functions for large-scale corporate, educational, and government networks. Supplementary services supported by Cisco IOS platforms are described in the “Common QSIG Implementation Considerations” topic.

A PISN provides telecommunications services to a specific set of users on a PISN Exchange (PINX). A PINX can be represented by a PBX, an Integrated Services CENTREX (ISCTX), or other equipment performing the following functions:

- Telecommunication services within its own area
- Telecommunication services from the public ISDN or PSTN
- Telecommunication services between PINXs in a multisite private network

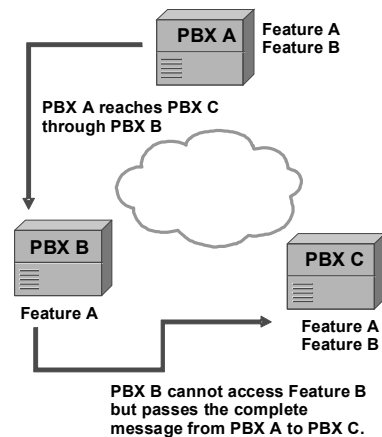
# QSIG Protocol

Cisco.com

## Some reasons for Q.SIG

- Feature Transparency
- Innovation for future networkability
- Guaranteed interoperability
- Flexible numbering plan
- Free-form network topology
- Flexible interconnection
- Multiapplication domain

## Feature Transparency

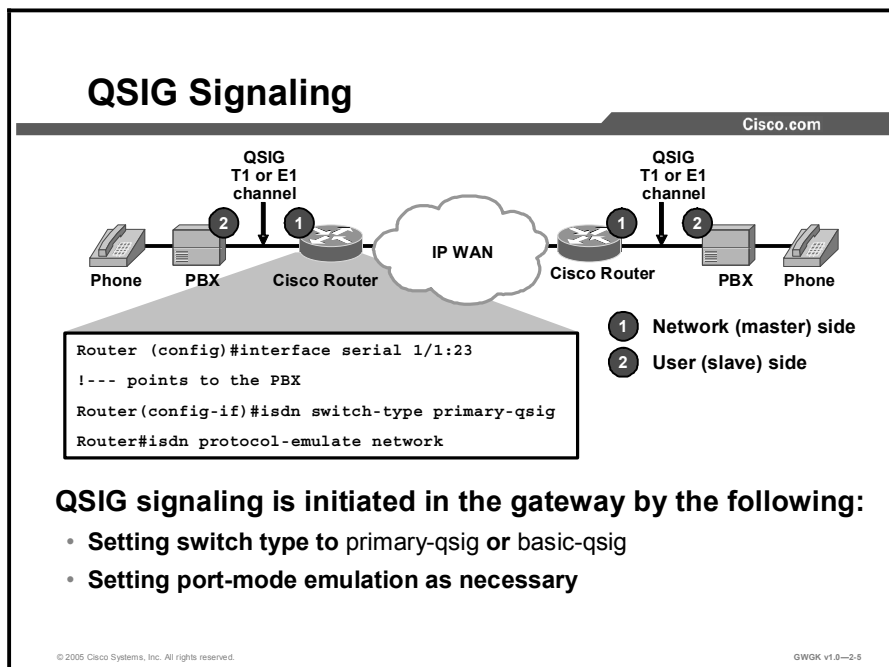


QSIG is recommended for some of the following reasons:

- **Feature transparency:** This is probably the most significant reason for choosing to use QSIG in a network. Not all PBXs in a network need to carry the same set of features. Each switch may offer different service levels through QSIG without any loss of features to the end destination. For instance, if PBX B (in the figure) does not fully support what PBX A has sent, but PBX C does, services from PBX A are transferred through PBX B and fully recognized at PBX C where those features can be served.
- **Innovation for future networkability:** Feature transparency allows vendors to develop supplementary services that can be transported within QSIG itself. For example, innovative services may be provided for site 1 and site 3 through PBX vendor A, but for site 2, the features are merely embedded within the packets and passed transparently through the corporate network.
- **Guaranteed interoperability:** The largest PBX manufacturers have agreed to ensure consistent support and development of QSIG.
- **Numbering plan flexibility:** QSIG provides enough flexibility to produce a detailed numbering plan that can include trunk access codes, office codes, directory numbers, area codes, and more.
- **Free-form topology:** QSIG does not restrict networks to one particular topology. QSIG can be a point-to-point, bus, star, or meshed type of network.
- **Interconnection flexibility:** QSIG allows for interconnection of a variety of network equipment. QSIG accounts for any transmission delays associated with a particular type of physical device or for software features such as Virtual Private Networks (VPNs).
- **Multiapplication domain:** QSIG can be implemented for PBX equipment and for other applications and peripherals in the corporate network such as fax servers, cordless control units, and data processing hardware to make them available to all users on the corporate telephone network (as determined by management and administrators).

# QSIG Signaling

This topic describes the QSIG switch types that are used on the network and user sides of voice-enabled topology.



QSIG enables Cisco voice gateways to emulate the functionality of the PSTN.

QSIG messages that originate and terminate on QSIG endpoints pass transparently across the network; the PBXs process and provision any supplementary services. When there is a mix of QSIG and non-QSIG endpoints, only basic calls that do not require supplementary services are supported.

QSIG signaling is initiated on a voice gateway after you identify the basic or primary QSIG switch type for the switch in global-configuration mode or for an interface in interface-configuration mode. Once you have identified the switch type, the network and user sides must be established to determine which endpoint on a link will be master and which will be slave. Typically, the master node provides clocking. Configuration at this point is identical to the configuration for ISDN PRI.

# Common QSIG Implementation Considerations

This topic describes common QSIG issues during voice gateway deployment.

## Common QSIG Implementation Considerations

Cisco.com

### QSIG Standards supported

- ECMA 141, 142, 143(ETSI300-172), 165(ETSI239), and Q.SIG v1 and v2
- No IE for supplemental services are interpreted, but instead passed according to ECMA-165 with these exceptions:
  - No support for MULTIRATE
  - No support of facility IE for call-related RELEASE/RELEASE COMPLETE
  - No support of facility IE for connection-oriented RELEASE COMPLETE
- Overlap and enbloc signaling are supported

© 2005 Cisco Systems, Inc. All rights reserved.GWOK v1.0--2.6

QSIG implementation is similar to ISDN but, with its large supplementary services library and feature transparency, you are additionally required to consider what parts of QSIG are actually supported by Cisco platforms.

The QSIG standards that are supported in Cisco IOS software are listed in the figure. The Cisco platforms that support QSIG are as follows:

- **Cisco 2800 Series and 3800 Series Routers:** BRI and T1/E1 QSIG (as of 12.0.7XK/12.1.2T)
- **Cisco 7200 Series Routers:** T1/E1 QSIG (as of 12.0.7XK/12.1.2T)
- **Cisco 7500 Series Routers:** T1/E1 QSIG (as of 12.1.3T)
- **Cisco 5300 Series Access Servers:** T1/E1 (as of 12.0.7T)

---

**Note** Implementers should continue to follow the evolving support for QSIG on Cisco IOS platforms through the product datasheets and the Cisco.com PBX Interoperability Portal.

---

Many of the messages and information elements supported in ISDN are supported in QSIG. The “QSIG Message Supported by Cisco IOS” table lists the QSIG messages and information elements (IEs) that are supported by Cisco IOS.

## QSIG Messages Supported by Cisco IOS Software

| QSIG Basic Call Messages                                                                                                                                                                                    | QSIG Supplementary Services Messages    | QSIG Information Elements                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SETUP<br>SETUP ACK<br>ALERTING<br>PROCEEDING<br>CONNECT<br>CONNECT ACK<br>PROGRESS<br>DISCONNECT<br>RELEASE<br>RELEASE COMPLETE<br>RESTART<br>RESTART ACK<br>SEGMENT<br>INFORMATION<br>STATUS<br>STATUS INQ | FACILITY<br>NOTIFY<br>USER-USER MESSAGE | Sending complete<br>Codeset shift<br>Segmented message<br>Bearer cap<br>Cause<br>Call state<br>Channel ID<br>Progress indicator<br>Connected number<br>Connected subaddress<br>Calling party<br>Calling party subaddress<br>Called party<br>Called party subaddress<br>Restart indicator<br>Lower layer compatibility<br>Higher layer compatibility<br>Facility<br>Notify indicator<br>User-user (for Ericsson MD110)<br>Codeset 5: Party category and transit counter<br>Codeset 7: User-user (for Alcatel) |

Along with the messages shown in the table, Cisco IOS supports the following supplementary services:

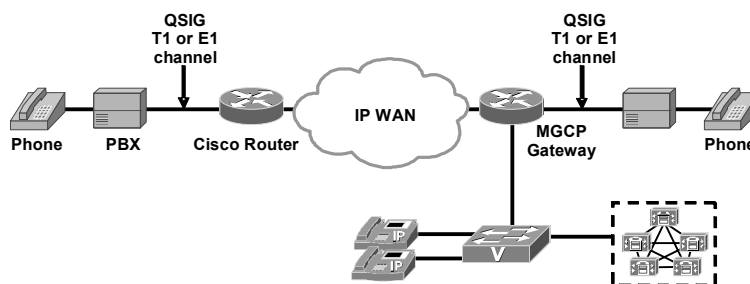
- Identification services:
  - Calling line and calling name ID with presentation or restriction (calling line identification presentation [CLIP], calling line identification restriction [CLIR] calling name identification presentation [CNIP], calling name identification restriction [CNIR]) as described in the following ECMA specifications—ECMA 148, 163, and 164
  - Connected line and connected name ID and presentation (connected line identification presentation [COLP], connected name identification presentation [CONP])—ECMA 163, and 164
- Call forward unconditional (CFU), call forward busy (CFB), and call forward no reply (CFNR) as described in ECMA 173 and 174
- Call transfer (CT)—ECMA 177 and 178
- Path replacement—ECMA 175 and 176
- Call completion—ECMA 185, and 186
- Call offer (CO)—ECMA 191 and 192
- Do not disturb or do not disturb override—ECMA 193 and 194
- Call intrusion—ECMA 202 and 203



- Advice of charge—ECMA 211 and 212
- Recall—ECMA 213 and 214
- Call interception—ECMA 220 and 221
- User to user signaling
- Subaddressing

## QSIG Implementation with Cisco CallManager

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.7

To implement the QSIG protocol with Cisco CallManager, the gateway must run in Media Gateway Control Protocol (MGCP) mode. Once you configure MGCP, you can setup the supplementary services. The most common supplementary services used with CallManager are identification services, Message Waiting Indicator (MWI) services, call diversion, and call transfer.

---

**Note** Details on PBX and gateway configurations are provided on Cisco.com at the PBX Interoperability portal.

---

### Identification Services

Cisco voice gateways and Cisco CallManager provide configuration settings to control the following caller line ID (CLID) and caller name (CNAM) information on phone displays:

- CLIP or CLIR: Display or restrict the calling number
- CNIP or CNIR: Display or restrict the calling name
- COLP or COLR: Display or restrict the number of the connected line
- CONP or connected name identification restriction (CONR): Display or restrict the name of the connected party

Cisco CallManager Administration provides flexible configuration options to control the display of caller ID information. You can allow or restrict the display of this information for all calls by using fields in the Gateway Configuration window, or you can control the display of this information on a call-by-call basis by using fields in the Route Patterns and Translation Patterns windows. For information about configuring QSIG identification services, see the “Caller Identification and Restriction” topic.

## Message Waiting Indication Services

In a QSIG network, when a PINX has a connected voice-messaging system that services users in another PINX, the message center PINX can send the following MWI signals to the other PINX:

- **MWI Activate:** Send a signal to another PINX to activate MWI on the served user phone after the voice-messaging system receives a message for that phone.
- **MWI De-Activate:** Send a signal to deactivate the MWI after the user has listened to messages in the associated voice-messaging system.

---

**Note** Cisco CallManager does not support the MWI interrogation service.

---

A PINX that is not a message center can receive the following MWI signals and perform the associated functions:

- **MWI Activate:** Receive a signal from another PINX to activate MWI on the served user phone.
- **MWI De-Activate:** Receive a signal to deactivate the MWI on the served user phone.

If the voice-messaging system is connected to Cisco CallManager using QSIG connections or using the Cisco Messaging Interface (CMI), the MWIs are set based on QSIG directives.

When a call is forwarded to another number and then diverted to a voice-messaging system, QSIG supplementary services can provide the information to place the voice message in the originally called party voice mailbox.

The MWI service uses the existing dial number that is set up in Cisco CallManager Administration for message waiting and does not require any additional configuration.

## Call Diversion (Forwarding)

The QSIG standards describe two methods for call diversion: Call diversion by reroute and call diversion by forward switching. Cisco CallManager supports call diversion by forward switching only.

QSIG diversion supplementary services provide call forwarding capabilities that are similar to the familiar Cisco CallManager call forwarding features. The user or the system administrator can activate any of these features on individual directory numbers. Call forwarding supplementary services include the following:

- **Supplementary services (SS)-CFU:** Diverts all calls for a directory number (DN) to another DN. In Cisco CallManager, this feature is call forward all (CFA)
- **Supplementary services (SS)-CFB:** Diverts calls for a directory number to a predefined destination number when the directory number is busy. In Cisco CallManager, this feature is CFB
- **Supplementary services (SS)-CFNR:** Diverts calls for a directory number to another destination number when the directory number does not answer within a predefined time. In Cisco CallManager, this feature is call forward no answer (CFNA).

---

**Note** Supplementary services call deflection (SS-CD): Allows the user to respond to an incoming call by selectively diverting the call to another number. CD is not supported by QSIG or Cisco CallManager.

---

QSIG provides information to the originating PINX about the status and destination of outbound calls. To provide feature transparency with other PBXs in the network, information about a forwarded call is passed during the call setup and connection over QSIG trunks. Phone displays can present calling name or calling number or both, and called name or number or both, to show the destination of the forwarded call.

When calls are forwarded between multiple PINXs, a forwarding loop can result. A hop counter limits this possibility of calls getting caught in a looping condition. A hop counter also prevents you from having to enter a long forwarding chain. Configure the Forward Maximum QSIG Hop Count parameter in Cisco CallManager service parameters.

QSIG supplementary services provide the information to place the voice message from a diverted call in the originally called-party voice mailbox.

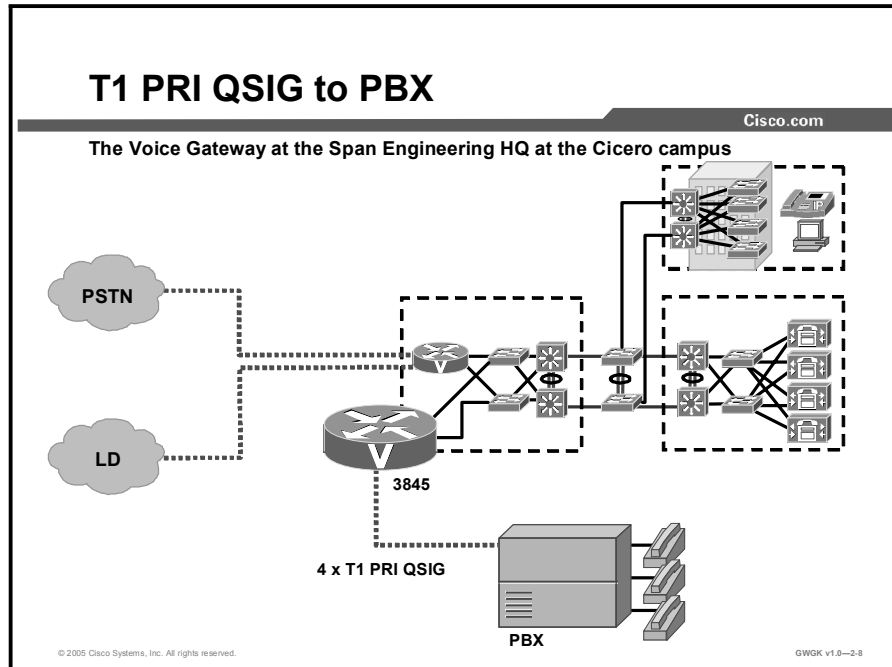
## **Call Transfer**

The QSIG standards describe two methods for transferring calls: Call transfer by reroute and call transfer by join. Cisco CallManager provides for call transfer over QSIG trunks by join only.

When a user transfers a call to another user, QSIG identification service provides for changing the connected name and number on the transferred party phone display. Call transfer requires no additional configuration in Cisco CallManager Administration.

# Common QSIG Gateway Configuration Examples

This topic describes how to configure a gateway to support QSIG connections.



The “Configure PRI for QSIG” table provides a description of the steps required to configure PRIs for QSIG.

## Configure PRI for QSIG

| Step | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Enter controller configuration mode for the specified controller.<br><br>Router(config)#<br><b>controller</b> {t1   e1}<br><i>controller-number</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Enter the controller as E1 or T1, and enter a <i>slot/port</i> location on Cisco routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 2.   | Configure the PRI group for either T1 or E1.<br><br>Router(config-controller)# <b>pri-group timeslot</b> <i>timeslot-range</i><br><br>NFAS configuration commands are as follows:<br><ul style="list-style-type: none"> <li>■ For primary D channel on one controller<br/><b>pri-group timeslot 1-24 nfas_d primary nfas_int number nfas_group number</b></li> <li>■ For backup D channel on a second controller<br/><b>pri-group timeslot 1-24 nfas_d backup nfas_int number nfas_group number</b></li> <li>■ For 24 B channels on third controller<br/><b>pri-group timeslot 1-24 nfas_d none nfas_int number nfas_group number</b></li> </ul> | <i>timeslot-range</i> is the range of timeslots that make up the PRI group. T1 range is 1 to 23. E1 range is 1 to 31.<br><br>The PRI group can include all or a select group of available timeslots.<br><br>For an NFAS configuration, the following tasks are done: <ul style="list-style-type: none"> <li>■ On one channelized T1 controller, configure the NFAS primary D channel.</li> <li>■ On a different channelized T1 controller, configure the NFAS backup D channel that is to be used if the primary D channel fails.</li> <li>■ On other channelized T1 controllers, configure a 24 B channel interface, if desired. (Optional)</li> </ul> |
| 3.   | Enter interface configuration mode for the ISDN PRI interface and the specified interface slot and port location and channel number.<br><br>Router(config)#<br><b>interface serial</b><br><i>slot/port:channel-number</i>                                                                                                                                                                                                                                                                                                                                                                                                                        | Enter a <i>slot</i> number from 1 to 6 and a <i>port</i> number of 1 or 2. For T1, enter the channel number as 23. For E1, enter the channel number as 15.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 4.   | If you did not configure the global PRI ISDN switch type for QSIG support in global configuration mode, configure the interface ISDN switch type to support QSIG signaling.<br><br>Router(config-if)# <b>isdn switch-type primary-qsig</b>                                                                                                                                                                                                                                                                                                                                                                                                       | For this interface, this command overrides the setting of the <b>isdn switch-type</b> command entered in global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 5.   | Router(config-if)# <b>isdn contiguous-bchan</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | (E1 only) Specifies contiguous B channel handling so that B channels 1 to 30 map to timeslots 1 to 31 and skip timeslot 16.<br><br>This command was added to allow interoperability with Siemens PBXs, which number the B channels consecutively from 1 to 30 instead of from 1 to 15 and 17 to 31.                                                                                                                                                                                                                                                                                                                                                     |

| Step | Action                                                                                                                                                                                                    | Notes                                                                                                                                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.   | Configure the Layer 2 and Layer 3 port protocol emulation.<br>Router(config-if)# <b>isdn protocol-emulate</b> { <b>user</b>   <b>network</b> }                                                            | <b>user</b> : Configures the port as TE; the PINX is the master. This is the default. The term "user" is equivalent to the QSIG term "slave".<br><b>network</b> : Configures the port as NT; the PINX is the slave. The term network is equivalent to the QSIG term <i>master</i> .         |
| 7.   | (Optional) Activate overlap signaling to send to the destination PBX.<br>Router(config-if)# <b>isdn overlap-receiving</b> <i>value</i>                                                                    | In this mode, the interface waits for possible additional call-control information from the preceding PINX.<br>The default mode is <i>enbloc</i> , in which all call establishment information is sent in the setup message without a need for additional messages from the preceding PINX. |
| 8.   | (Optional) Specify the cause code to pass to the PBX when a call cannot be placed or completed because of internal network failures.<br>Router(config-if)# <b>isdn network-failure-cause</b> <i>value</i> | The possible value range is 1 to 127.                                                                                                                                                                                                                                                       |

The following is an example excerpt for Span Engineering headquarters PBX connectivity as shown in the figure.

```
Router(config)#show running configuration
!---entire configuration is not shown, just those parts relevant to
!---PRI QSIG.
 isdn switch-type primary-qsig
 !
 controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d primary nfas_int 1 nfas_group 1
 !
 controller T1 1/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d none nfas_int 2 nfas_group 1
 !
 controller T1 2/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d backup nfas_int 3 nfas_group 1
 !
 controller T1 2/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 nfas_d none nfas_int 4 nfas_group 1
 !
 interface Serial1/0:23
 no ip address
```

```

no logging event link-status
isdn incoming-voice voice
isdn T310 60000
no cdp enable
!
interface Serial1/1:23
no ip address
no logging event link-status
isdn incoming-voice voice
isdn T310 60000
no cdp enable
!
interface Serial2/0:23
no ip address
no logging event link-status
isdn incoming-voice voice
isdn T310 60000
no cdp enable
!
interface Serial2/1:23
no ip address
no logging event link-status
isdn incoming-voice voice
isdn T310 60000
no cdp enable
!
voice-port 1/0:23
!
voice-port 1/1:23
!
voice-port 2/0:23
!
voice-port 2/1:23
!
dial-peer cor custom
!
dial-peer voice 1000 voip
destination-pattern 777444....
session target ipv4:10.0.0.2
!
dial-peer voice 100 pots
destination-pattern 777222....
direct-inward-dial
port 1/0:23
!
dial-peer voice 2 pots
destination-pattern 2222
port 4/0/0

```



# Troubleshooting QSIG Circuits

This topic describes how to use troubleshooting tools to resolve QSIG issues.

## Troubleshooting QSIG Circuits

Cisco.com

**In addition to common ISDN issues, QSIG considerations include the following:**

- **QSIG basic call**
- **Identification services**
- **MWI services**
- **Call diversion (forwarding)**
- **Call transfer**

For specific PBX vendor-related issues on QSIG, visit the PBX Interoperability Portal at [http://www.cisco.com/warp/public/779/largeent/avid/inter\\_operability/flash/portal.html](http://www.cisco.com/warp/public/779/largeent/avid/inter_operability/flash/portal.html).

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0—2.9

The “QSIG Troubleshooting Commands” table provides a description of helpful troubleshooting commands.

## QSIG Troubleshooting Commands

| Command                                       | Purpose                                                                                                                                                                                                                                                                    |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show isdn status</b>               | Displays the status of all ISDN interfaces, including active layers, timer information, and switch type settings                                                                                                                                                           |
| Router# <b>show controllers {t1   e1}</b>     | Displays information about T1 and E1 controllers                                                                                                                                                                                                                           |
| Router# <b>show voice port summary</b>        | Displays summary information about voice-port configuration                                                                                                                                                                                                                |
| Router# <b>show dial-peer voice</b>           | Displays how voice dial peers are configured                                                                                                                                                                                                                               |
| Router# <b>show cdapi</b>                     | Displays the call distributor application programming interface (CDAPI) information                                                                                                                                                                                        |
| Router# <b>show call history voice record</b> | Displays information about calls made to and from the router                                                                                                                                                                                                               |
| Router# <b>show rawmsg</b>                    | Displays information about any memory leaks                                                                                                                                                                                                                                |
| Router# <b>debug isdn event</b>               | This displays events occurring on the user side (on the router) of the ISDN interface. The ISDN events that can be displayed are Q.931 events (call setup and teardown of ISDN network connections).                                                                       |
| Router# <b>debug isdn q931</b>                | Displays information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network                                                                                                                              |
| Router# <b>debug tsp</b>                      | Displays information about the telephony service provider (TSP).                                                                                                                                                                                                           |
| Router# <b>debug cdapi {events   detail}</b>  | Displays information about CDAPI application events, registration, messages, and so on                                                                                                                                                                                     |
| Router# <b>debug voip ccapi inout</b>         | Traces the execution path through the call-control API, which serves as the interface between the call-session application and the underlying network-specific software. You can use the output from this command to understand how calls are being handled by the router. |

# Summary

This topic summarizes the key points discussed in this lesson.

## Summary

Cisco.com

- **At OSI Layer 1 and Layer 2, QSIG is the same as ISDN. At Layer 3 QSIG has three sub-layers, QSIG-BC, QSIG-GF, and QSIG-SS.**
- **QSIG is popular in private networks because of its feature transparency that allows developers to add supplementary services without having to worry about their affect on the whole network.**
- **QSIG signaling is easily set up by identifying the basic- or primary-qsig switch type in either the global configuration or interface configuration.**
- **Network-side port mode emulation should be set up in accordance with the master/slave relationship the PBX expects to see.**
- **PRI QSIG configurations are part of the isdn command set in Cisco IOS software. They differ from standard PRI or BRI configurations in switch type.**
- **QSIG troubleshooting follows the same procedures used to troubleshoot ISDN BRI and PRI.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-2.10

# 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) Describe why feature transparency is important for the proliferation of QSIG as the signaling agent for PBXs. (Source: QSIG Circuit Overview)

---

---

---

---

---

## Lesson Self-Check Answer Key

- Q1) Not all PBXs in a network need to carry the same set of features. Each switch may offer different service levels through QSIG without any loss of features to the end destination. This makes QSIG safe for the rollout of desired features in some places without worrying that other places in the network, or in other networks, will be compromised.

# Module Summary

This topic summarizes the key points discussed in this module.

## Module Summary

Cisco.com

- When integrating the PSTN and a PBX with voice gateways, pay special attention to how the legacy systems will be implemented or “rolled over” into a Cisco-based VoIP solution.
- Technician line testers, E&M rollover cables, and Cisco ISO voice debug commands are the key problem solving tools that mitigate the challenge of connecting a voice gateway to the PSTN or a PBX with analog circuits.
- Integrating a voice gateway to the PSTN or a PBX using CAS circuits requires a thorough knowledge of T1 and E1 R2 signaling. Cisco voice gateways support the fulfillment of 911 and E911 services over T1 CAS by supporting ANI information transmission using E&M-FGD and receiving ANI information using FGD-EANA .
- PRI offers many valued telephony services that can be lost if the voice gateway integration with the PSTN or a PBX is incorrect. ISDN cause codes prove enormously valuable in diagnosing ISDN service failures.
- QSIG is fast becoming the worldwide standard for PBX interoperability. Feature transparency allows all the devices that handle calls to activate just the features that they are able to. You want to know how many of these supplementary services your voice gateway can support and how you can extract the richest features possible from a network connection to a PBX.

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-2.1

As you prepare to integrate a voice gateway with the PSTN or with a PBX, remember that there are many factors that influence the success of that integration. One of those factors is the trunk that you will use to actually make the hook-up. As long as companies use analog fax machines and analog E911 phones, you will have to know about analog trunks. For those who want the features of PRI but find it too expensive, CAS provides good throughput at a reasonable cost. Finally, the variants of ISDN, including BRI, PRI, and Q Signaling (QSIG) take telephony into a world of advanced calling-name features and diagnostics capability. For all of these types of trunks, it is important to know how to coordinate with the service provider. In advance of getting the service, and once the service is in place, it is important to be able to configure it for operation in your network. Preparing yourself for success with your trunks ensures a more peaceful transition from the telephony environment you know to the one that you are getting to know.

## References

For additional information, refer to these resources:

### Analog Circuits

- *Analog E&M Troubleshooting Guidelines (Cisco IOS Platforms).*  
[http://www.cisco.com/en/US/tech/tk652/tk701/technologies\\_tech\\_note09186a0080093f5e.shtml](http://www.cisco.com/en/US/tech/tk652/tk701/technologies_tech_note09186a0080093f5e.shtml).
- *Cisco Systems Inc. Application Note: Analog CAMA Trunk Support on the 26/36/37xx Platforms.* [http://wwwin.cisco.com/access/mce/tech/docs/vicCAMA\\_apnote.doc](http://wwwin.cisco.com/access/mce/tech/docs/vicCAMA_apnote.doc).

- *Cisco High Density Analog Voice and Fax Network Module.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products\\_feature\\_guide09186a0800dcd01.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0800dcd01.html).
- *Understanding Foreign Exchange Station FXS Voice Interface Cards.*  
[http://www.cisco.com/en/US/tech/tk652/tk653/technologies\\_tech\\_note09186a0080094fac.shtml](http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a0080094fac.shtml).
- *Cisco VG 224 Analog Phone Gateway.*  
[http://www.cisco.com/en/US/products/hw/gatecont/ps2250/products\\_data\\_sheet09186a00801d87f6.html](http://www.cisco.com/en/US/products/hw/gatecont/ps2250/products_data_sheet09186a00801d87f6.html).
- *Cisco VG 248 Analog Phone Gateway.*  
[http://www.cisco.com/en/US/products/hw/gatecont/ps2250/products\\_data\\_sheet09186a008007c9bb.html](http://www.cisco.com/en/US/products/hw/gatecont/ps2250/products_data_sheet09186a008007c9bb.html).
- *IP Communications High-Density Digital Voice/Fax Network Modules for Cisco 2600XM/2691/2800/3700/3800.*  
[http://www.cisco.com/en/US/products/hw/modules/ps5365/products\\_data\\_sheet09186a0080191d41.html](http://www.cisco.com/en/US/products/hw/modules/ps5365/products_data_sheet09186a0080191d41.html).
- *Troubleshoot Analog FXO GroundStart Outbound Call Failures.*  
[http://www.cisco.com/en/US/tech/tk652/tk653/technologies\\_tech\\_note09186a00803736c1.shtml](http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00803736c1.shtml).
- *Trunk-Management Features.*  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/vcltrunk.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/vcltrunk.htm).

## Cisco Hardware

- *Cisco Systems Inc. Cisco Catalyst 6500 Series and Cisco 7600 Series Communication Media Module.* [http://wwwwin.cisco.com/cmc/cc/pd/ifaa/ps4633/prodlit/cmmrd\\_ds.htm](http://wwwwin.cisco.com/cmc/cc/pd/ifaa/ps4633/prodlit/cmmrd_ds.htm).
- *Cisco Systems Inc. FXO, FXS, and E&M Voice Card Interface Support on Cisco 1700 Series Routers.*  
[http://www.cisco.com/en/US/products/hw/routers/ps221/prod\\_configuration\\_guide09186a08019b16e.html](http://www.cisco.com/en/US/products/hw/routers/ps221/prod_configuration_guide09186a08019b16e.html).
- *Voice Hardware Compatibility Matrix.*  
[http://www.cisco.com/en/US/products/hw/routers/ps259/products\\_tech\\_note09186a00800e73f6.shtml](http://www.cisco.com/en/US/products/hw/routers/ps259/products_tech_note09186a00800e73f6.shtml).
- *Cisco Systems Inc. VG248 and VG224 Applications.*  
[http://wwwwin.cisco.com/access/mce/products/docs/VG248\\_VG224\\_applications.ppt](http://wwwwin.cisco.com/access/mce/products/docs/VG248_VG224_applications.ppt).

## IOS Command References

- *Important Information on Debug Commands.*  
[http://www.cisco.com/en/US/tech/tk801/tk379/technologies\\_tech\\_note09186a008017874c.shtml](http://www.cisco.com/en/US/tech/tk801/tk379/technologies_tech_note09186a008017874c.shtml).
- *Cisco IOS Debug Command Reference, Release 12.3.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products\\_command\\_reference\\_book09186a008017cf4d.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a008017cf4d.html).
- *Cisco IOS Software.* <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml>.

## IOS Voice

- *Cisco IOS Voice Command Reference, Release 12.3.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products\\_command\\_reference\\_book09186a00801e8a79.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_command_reference_book09186a00801e8a79.html).
- *Cisco IOS Voice Configuration Library.*  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vcl.htm>.
- *Cisco IOS Voice Troubleshooting and Monitoring Guide.*  
[http://cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax\\_c/voipt\\_c/index.htm](http://cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax_c/voipt_c/index.htm).
- *Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_book09186a0080080ada.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ada.html).

## ISDN

- *Capabilities of Typical ISDN Switches.*  
[http://www.cisco.com/en/US/tech/tk801/tk379/technologies\\_tech\\_note09186a0080093d6d.shtml](http://www.cisco.com/en/US/tech/tk801/tk379/technologies_tech_note09186a0080093d6d.shtml).
- *Cisco IOS ISDN Voice Configuration Guide.*  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax\\_c/isdnv\\_c/](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax_c/isdnv_c/).
- *Feature Group D Support.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps5013/products\\_feature\\_guide09186a00800dd70f.html#79466](http://www.cisco.com/en/US/products/sw/iosswrel/ps5013/products_feature_guide09186a00800dd70f.html#79466).
- *Cisco IOS Software Release 12.0 Dial Solutions Configuration Guide: Setting Up ISDN Basic Rate Service.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products\\_configuration\\_guide\\_chapter09186a0080087311.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a0080087311.html).
- *Cisco Systems Inc. ISDN Basic Rate Interface (BRI).*  
<http://www.in.cisco.com/cct/data/itm/wan/isdn/wtisbri.htm>.
- *Cisco Systems Inc. ISDN PRI QSIG Voice Signaling.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products\\_feature\\_guide09186a008008785f.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a008008785f.html).
- *ISDN BRI Troubleshooting Flowchart.*  
[http://www.cisco.com/warp/public/129/isdn\\_20602.html](http://www.cisco.com/warp/public/129/isdn_20602.html).
- *ISDN Switch Types, Codes, and Values.*  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/dbook/disdn.htm>.
- *Interoperability Portal.*  
[http://www.cisco.com/warp/public/779/largeent/avid/inter\\_operability/flash/portal.html](http://www.cisco.com/warp/public/779/largeent/avid/inter_operability/flash/portal.html).
- *Troubleshooting ISDN Connections.*  
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg\\_v1/tr1917.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1917.htm).
- Intel Corporation. *Global Call ISDN Technology Guide.*  
[http://resource.intel.com/telecom/support/releases/winnt/sr60pci/onldoc/htmlfiles/globalcall\\_for\\_isdn.html](http://resource.intel.com/telecom/support/releases/winnt/sr60pci/onldoc/htmlfiles/globalcall_for_isdn.html).



## QSIG

- *ISDN PRI QSIG Voice Signaling.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products\\_feature\\_guide09186a08008785f.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1830/products_feature_guide09186a08008785f.html).
- *PRI and BRI QSIG Protocol Support on Cisco 2600, 3600, and MC3810 Series Routers and PRI QSIG on the Cisco 7200.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products\\_feature\\_guide09186a0800800b0.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0800800b0.html).
- *QSIG Backhaul (RUDP based) for Cisco IOS Gateways.*  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products\\_feature\\_guide09186a0800b5dab.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0800b5dab.html).
- *QSIG Feature Transparency.*  
[http://www.cisco.com/en/US/products/sw/voicesw/ps1913/products\\_feature\\_guide09186a08022c13d.html](http://www.cisco.com/en/US/products/sw/voicesw/ps1913/products_feature_guide09186a08022c13d.html).
- *Support of QSIG/Q.931 Over BRI Backhaul.*  
[http://www.cisco.com/en/US/products/sw/voicesw/ps1913/products\\_feature\\_guide09186a0801eefb7.html](http://www.cisco.com/en/US/products/sw/voicesw/ps1913/products_feature_guide09186a0801eefb7.html).

## T1 CAS

- *T1 Troubleshooting.*  
[http://www.cisco.com/en/US/tech/tk713/tk628/technologies\\_tech\\_note09186a00800a5f40.shtml](http://www.cisco.com/en/US/tech/tk713/tk628/technologies_tech_note09186a00800a5f40.shtml).
- *Configuring and Troubleshooting T1 CAS Signaling.*  
[http://www.cisco.com/en/US/tech/tk652/tk653/technologies\\_troubleshooting\\_procedures09186a00801040bc.shtml#configs](http://www.cisco.com/en/US/tech/tk652/tk653/technologies_troubleshooting_procedures09186a00801040bc.shtml#configs).
- *E1 R2 Customization with the cas-custom Command.*  
[http://www.cisco.com/en/US/tech/tk652/tk653/technologies\\_tech\\_note09186a00800942f2.shtml](http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800942f2.shtml).
- *E1 R2 Signaling Configuration and Troubleshooting.*  
[http://www.cisco.com/en/US/tech/tk652/tk653/technologies\\_configuration\\_example09186a00800ad389.shtml](http://www.cisco.com/en/US/tech/tk652/tk653/technologies_configuration_example09186a00800ad389.shtml).
- *E1 R2 Signaling for the Cisco 3620 and 3640 Series Routers.*  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/3600\\_r2.htm#wp3913](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/3600_r2.htm#wp3913).
- *E1 R2 Signaling Theory.*  
[http://www.cisco.com/en/US/tech/tk652/tk653/technologies\\_tech\\_note09186a00800943c2.shtml](http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800943c2.shtml).
- *E1 Troubleshooting.*  
[http://www.cisco.com/en/US/tech/tk713/tk628/technologies\\_tech\\_note09186a00800a70fb.shtml](http://www.cisco.com/en/US/tech/tk713/tk628/technologies_tech_note09186a00800a70fb.shtml).
- *Understanding How Digital T1 CAS (Robbed Bit Signaling) Works in IOS Gateways.*  
[http://www.cisco.com/en/US/tech/tk652/tk653/technologies\\_tech\\_note09186a00800e2560.shtml](http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800e2560.shtml).
- *VoIP with Channel Associated Signaling (CAS).*  
[http://www.cisco.com/en/US/tech/tk652/tk653/technologies\\_configuration\\_example09186a00800fa115.shtml](http://www.cisco.com/en/US/tech/tk652/tk653/technologies_configuration_example09186a00800fa115.shtml).



## 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 digit 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

© 2005 Cisco Systems, Inc. All rights reserved. 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.**

© 2005 Cisco Systems, Inc. All rights reserved.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 need 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 numbering 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 v1.0-3-8

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:

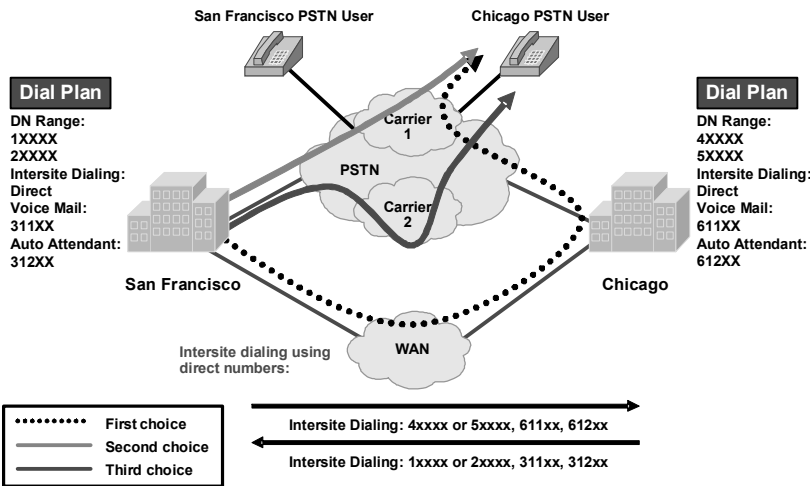
- **Dial-Plan Distribution:** Good dial-plan architecture relies on effectively distributing the dial-plan logic among the gateway and gatekeeper components. Isolating H.323 devices to a specific portion of the dial plan reduces the complexity of the configuration. Each component can focus on accomplishing 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 Scalable Dial Plan (Cont.)

Cisco.com



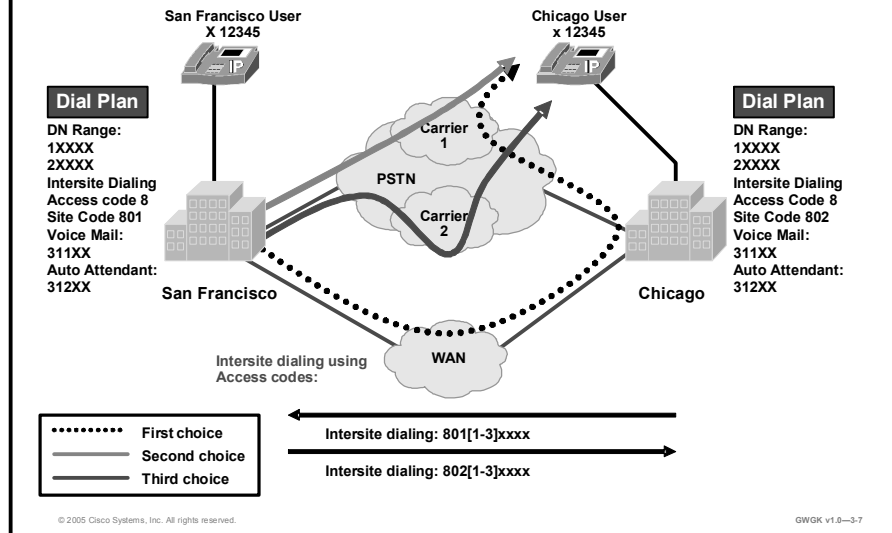
© 2005 Cisco Systems, Inc. All rights reserved.

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

Cisco.com



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.

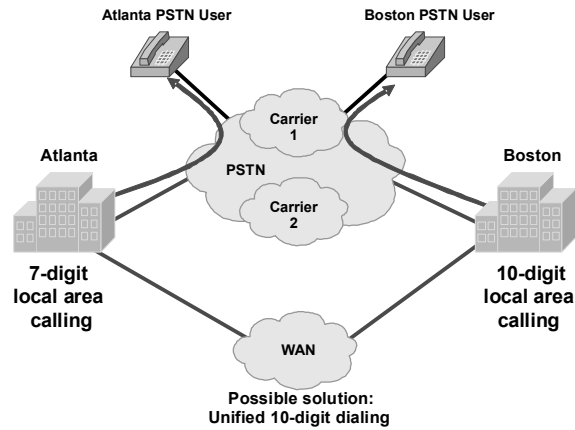
The access code selected for intersite dialing should be different from the access code used for off-net calling. If you use the same access code, you will need to make sure your intersite calls can be distinguished from off-net calls. This can lead to a very complicated dial plan. In the United States, 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 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 Scalable Dial Plan (Cont.)

Cisco.com

### 7-digit versus 10-digit dialing



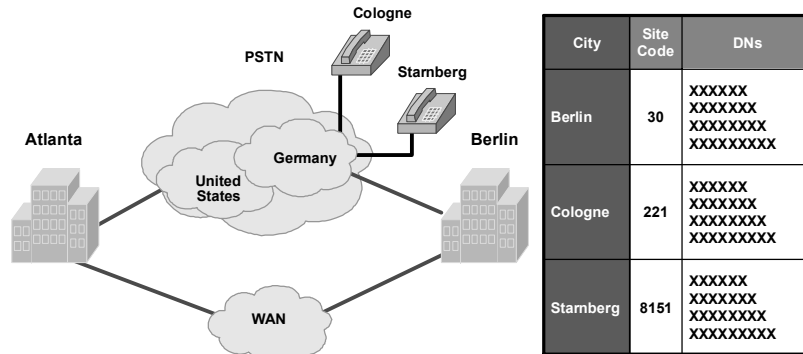
© 2005 Cisco Systems, Inc. All rights reserved.

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 Scalable Dial Plan (Cont.)

Cisco.com



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

© 2005 Cisco Systems, Inc. All rights reserved.

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.**

© 2005 Cisco Systems, Inc. All rights reserved. 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/voicesw/ps556/products_implementation_design_guide_chapter09186a00802c37f9.html)
- [http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a0080080aec.html#wp1241391](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 plans 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**

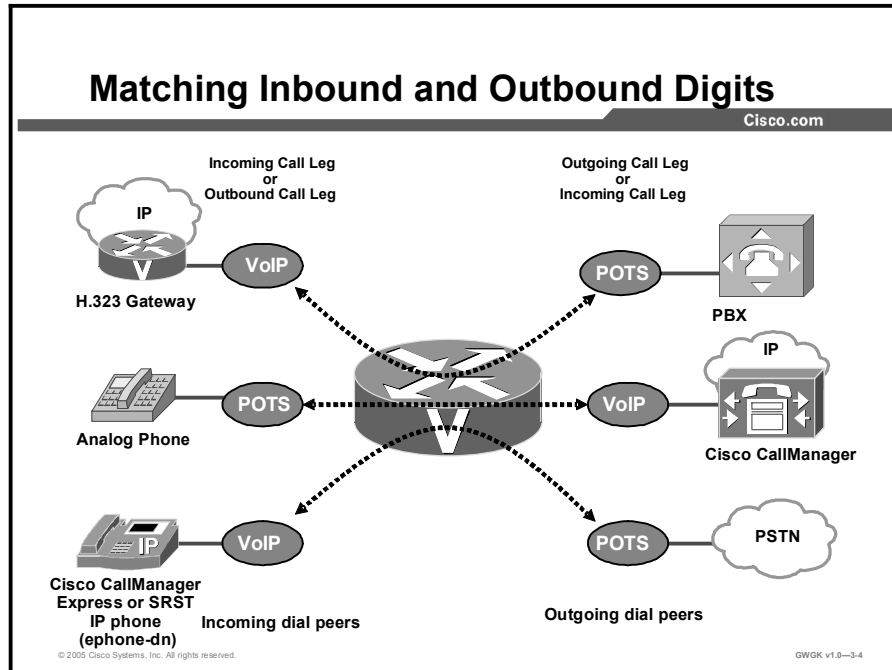
|                          |                                   |
|--------------------------|-----------------------------------|
| – prefix                 | (after outbound dial peer match)  |
| – forward-digits         | (after outbound dial peer match)  |
| – num-exp                | (before outbound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

© 2005 Cisco Systems, Inc. All rights reserved. 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.



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 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.

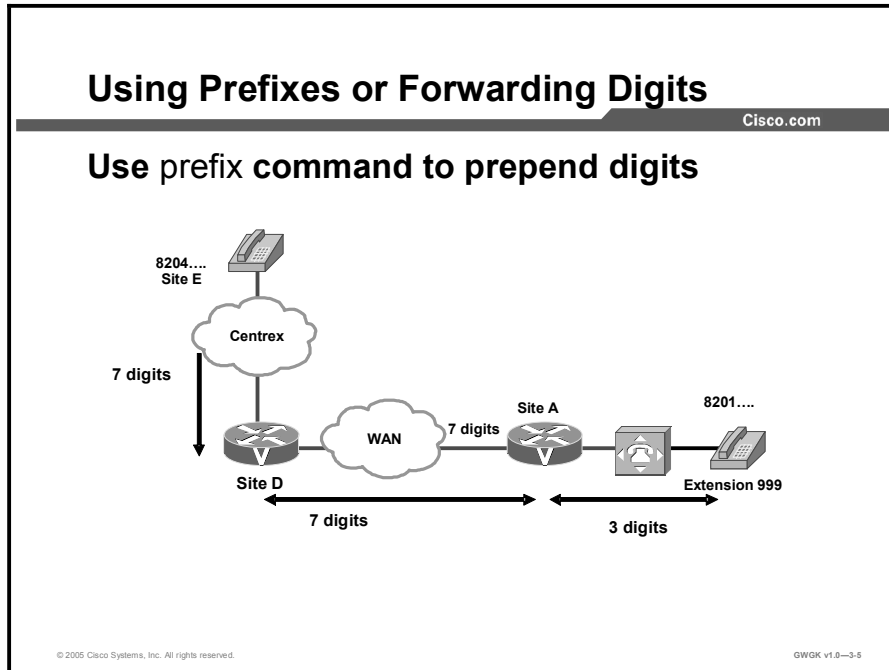
If no inbound peer can be matched using any of the criteria already listed, then the inbound peer is set to dial peer 0. The characteristics of dial peer 0, also seen as **peer ID = 0** in **debug voice ccapi inout**, is as follows:

- 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.



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.

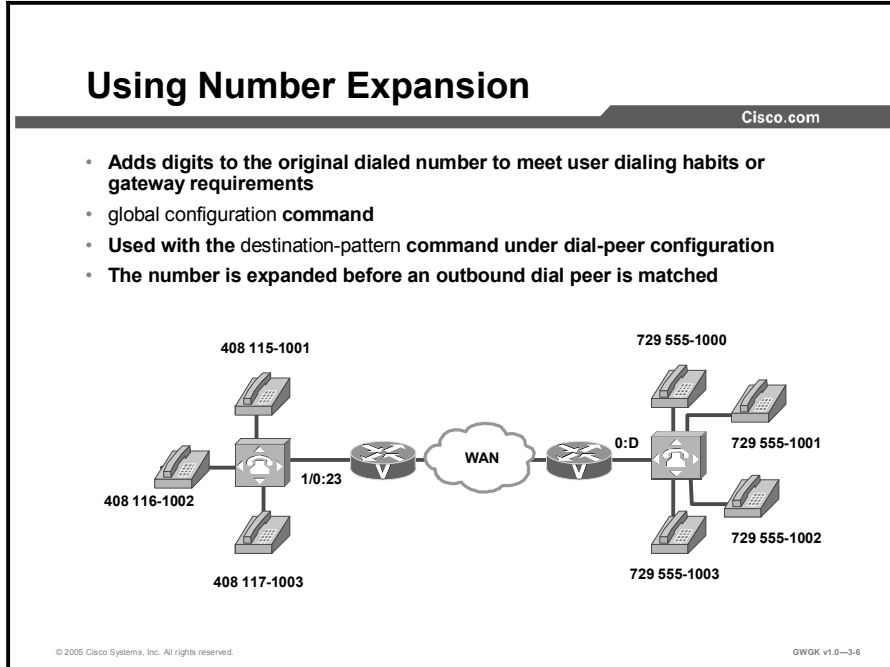
Calls in the reverse direction are handled similarly at Site A, but because the Centrex service requires the full seven-digit dial string to complete calls, the POTS dial peer at Site D is configured with no-digit stripping. Alternatively, digit stripping could be enabled and the dial peer could be configured 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 command 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.



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

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-3.7

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.

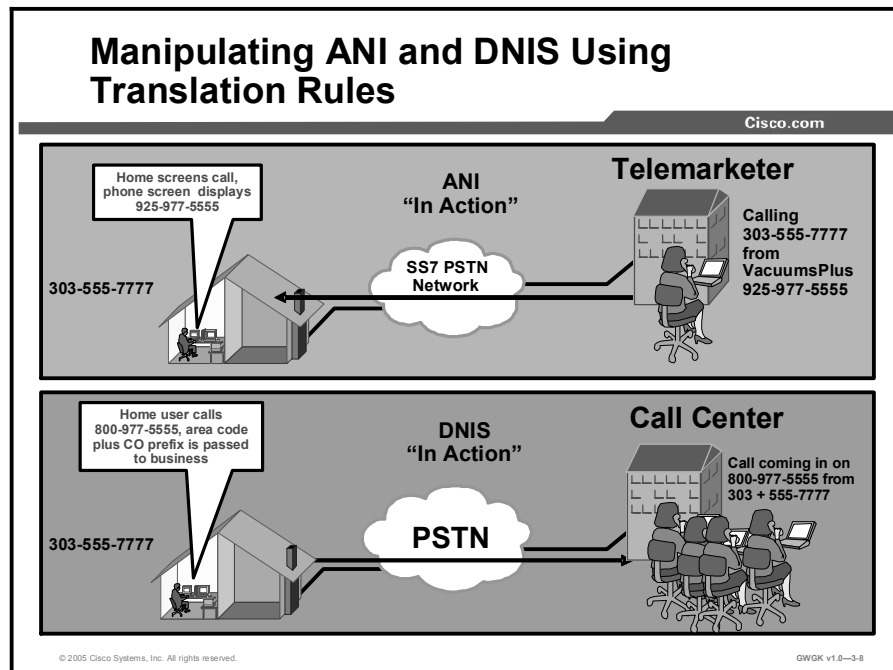
```
HQGW(config-dial-peer)#clid strip
HQGW#show dialplan number 914085551234
Macro Exp.: 914085551234

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).

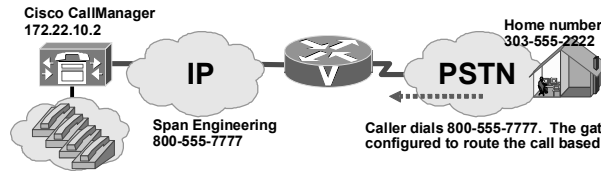


ANI identifies the telephone number of the calling party. The service provider provides this information. In the example in the figure, a telemarketer calls a home number, and the resident screens the call. The resident can see where the number is coming from and can decide to answer the call or not. 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



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
```

© 2005 Cisco Systems, Inc. All rights reserved.

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

| <h2 style="text-align: center;">Translation Rule Regular Expressions (Cont.)</h2> |                |                                        |                                        |                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------|----------------|----------------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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<br>555121212                | 9195553434<br>555123434                | Match end of string                                                                                                                                                                 |
| /^(^*)1212/                                                                       | /13434/        | 9195551212<br>555121212<br>55512121277 | 9195553434<br>555123434<br>55512343477 | No comment<br>Infinite length in front is why string is matched from right to left<br>Still matched from right to left, but because no \$, anything behind first occurrence is kept |
| /444/                                                                             | /555/          | 4441212<br>44441212<br>44414441212     | 5551212<br>55541212<br>55514441212     | Match substring                                                                                                                                                                     |

© 2005 Cisco Systems, Inc. All rights reserved. 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**

© 2005 Cisco Systems, Inc. All rights reserved.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 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.

© 2005 Cisco Systems, Inc. All rights reserved.

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
```

© 2005 Cisco Systems, Inc. All rights reserved. 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 **test 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
```

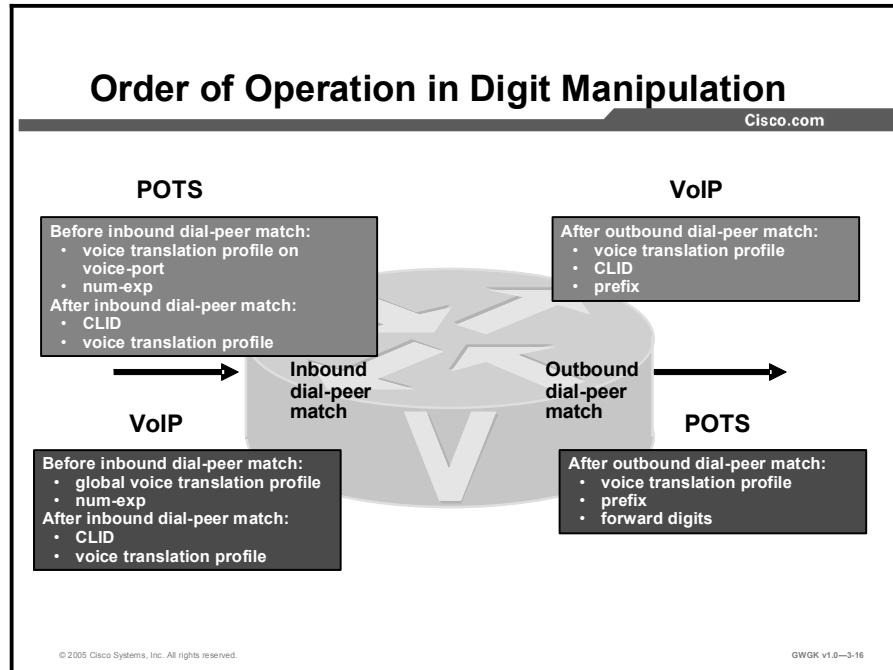
```
Replace type: none
```

```
Match plan: none
```

```
Replace plan: none
```

# Order of Operation in Digit Manipulation

This topic describes the order of operation in digit manipulation.



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](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](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/cgi-bin/Support/browse/psp\\_view.pl?p=Technologies:Voice\\_Call\\_Routing\\_Dial\\_Plans&view\\_all=true](http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Technologies:Voice_Call_Routing_Dial_Plans&view_all=true)
- Voice Translation Rule:  
[http://www.cisco.com/en/US/tech/tk652/tk90/technologies\\_tech\\_note09186a0080325e8e.shtml](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.

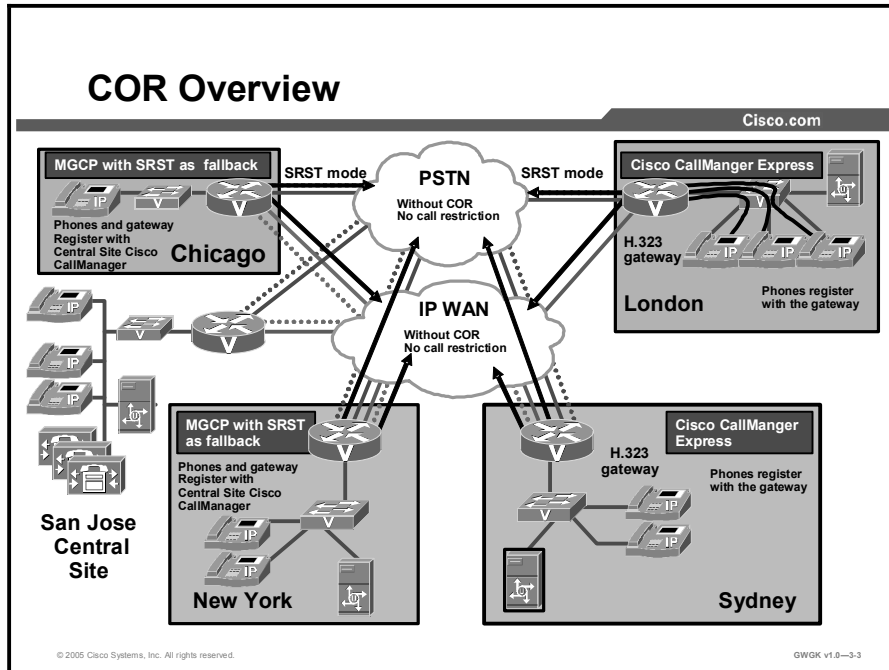
## Objectives

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.



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:

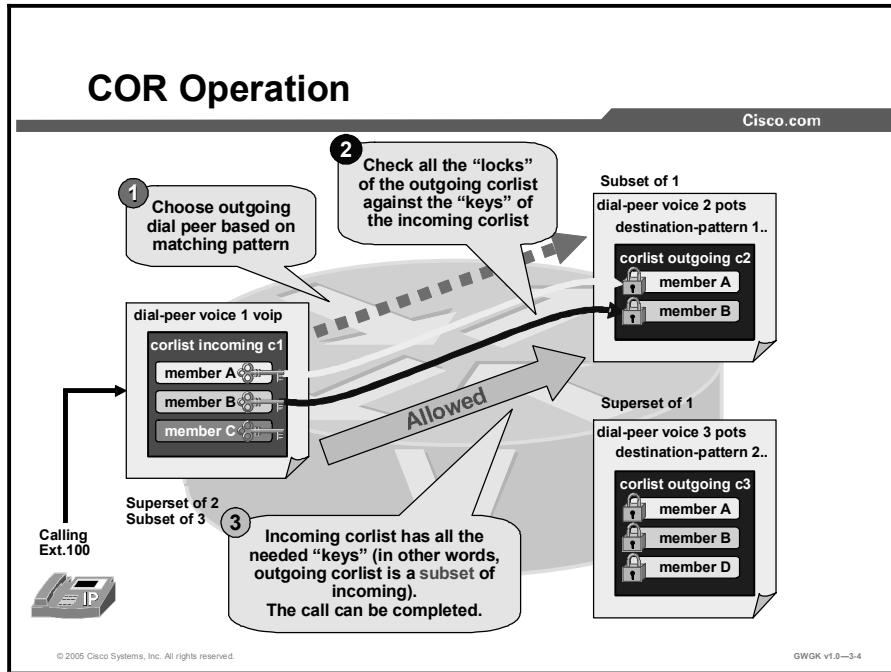
- One is when users at the MGCP lose communication with the Cisco CallManager at the central site and fall back to SRST mode. Without the central site CallManager managing their calling behavior, users can potentially have unlimited access to the PSTN.
- The other exists at the Cisco CallManager Express. 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

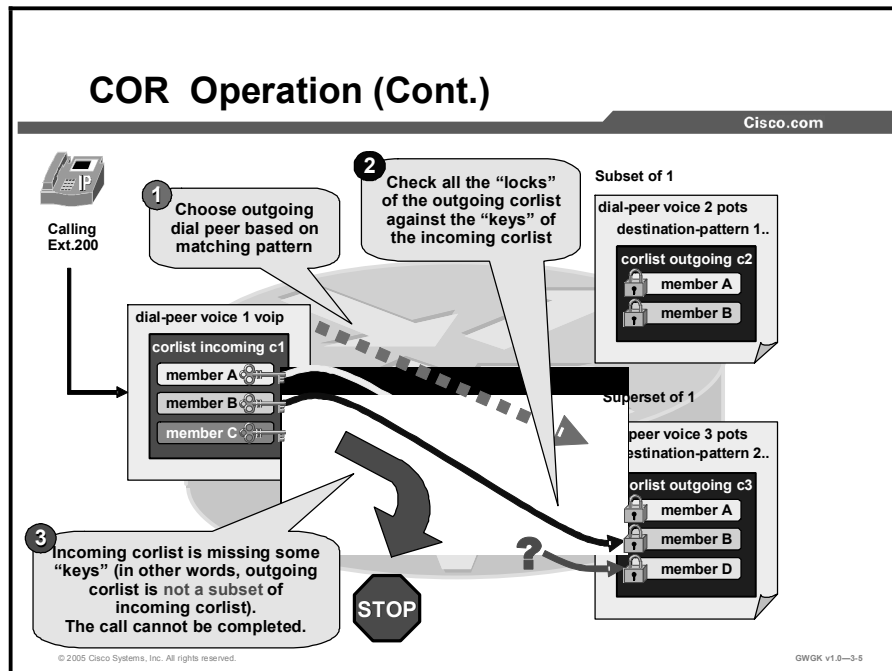
This topic describes COR operation and logic.



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.)

Cisco.com



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 <i>not</i> a super set of COR lists for outgoing calls on the outgoing dial peer.                                                                                     |

© 2005 Cisco Systems, Inc. All rights reserved.

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

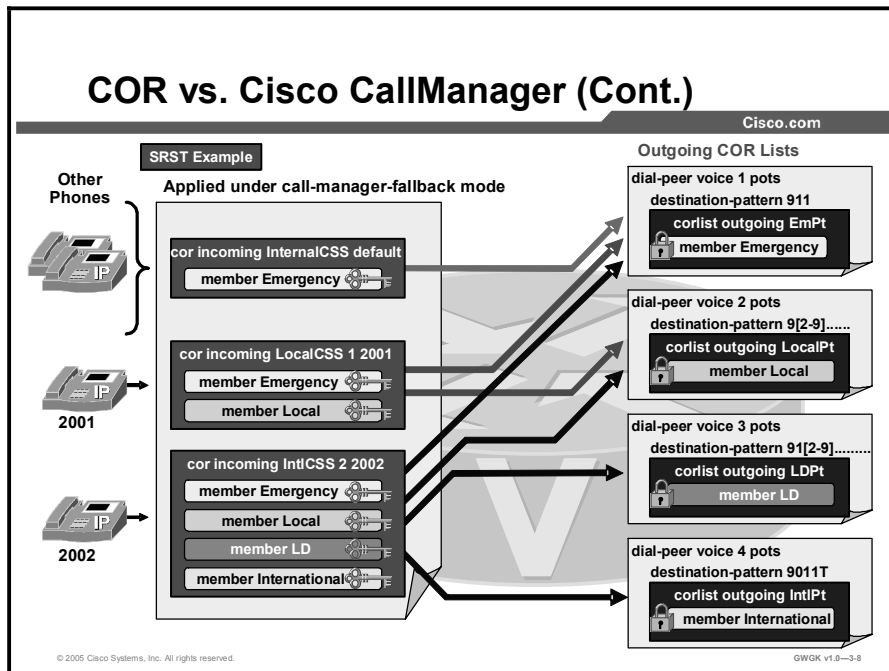
Cisco.com

- **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.**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.8--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.)



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.)

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

```
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)

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-3-10

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

Cisco.com

### 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

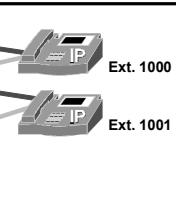
ephone-2 Mac:000F.2398.4533 TCP socket:[-1] activeLine:0 UNREGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:172.16.1.4 51577 Telecaster 7960 keepalive 1 max_line 6
button 1: dn 2 number 1001 CH1 IDLE CH2 IDLE
```

### 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
```



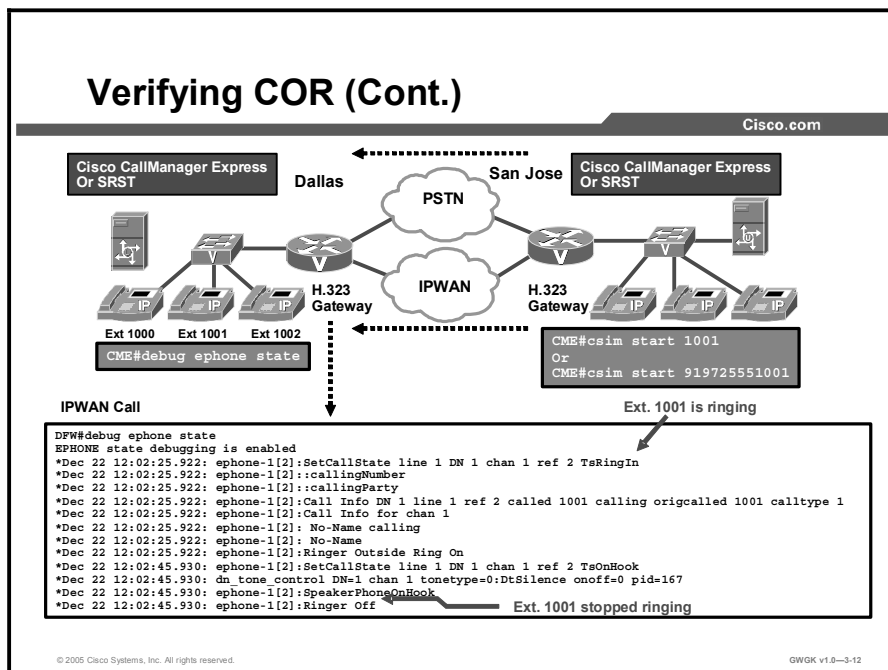
© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-3-11

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.)



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.**

© 2005 Cisco Systems, Inc. All rights reserved.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](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 priority
  - 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.

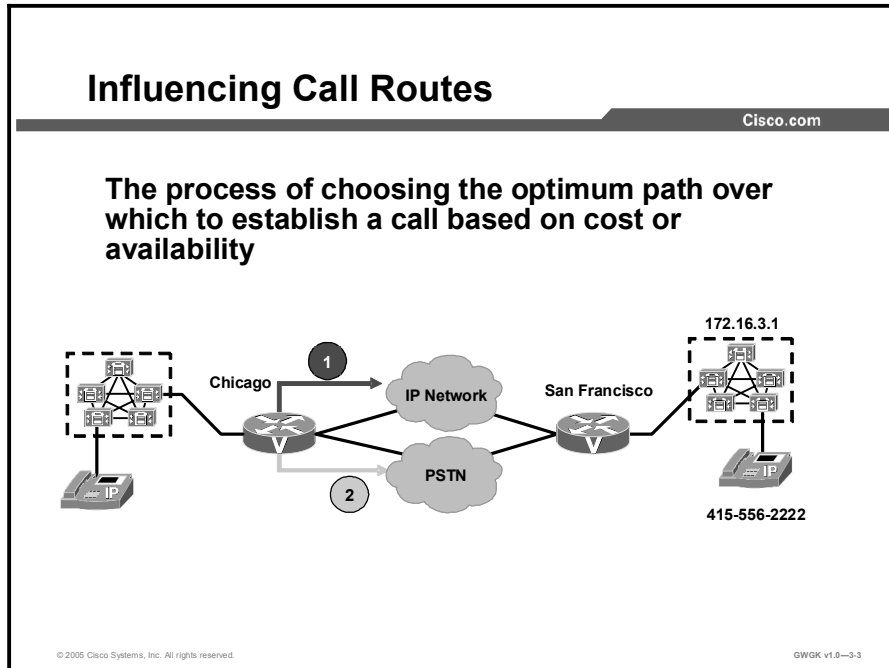
## Objectives

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.



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.**



**Without**

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



**With**

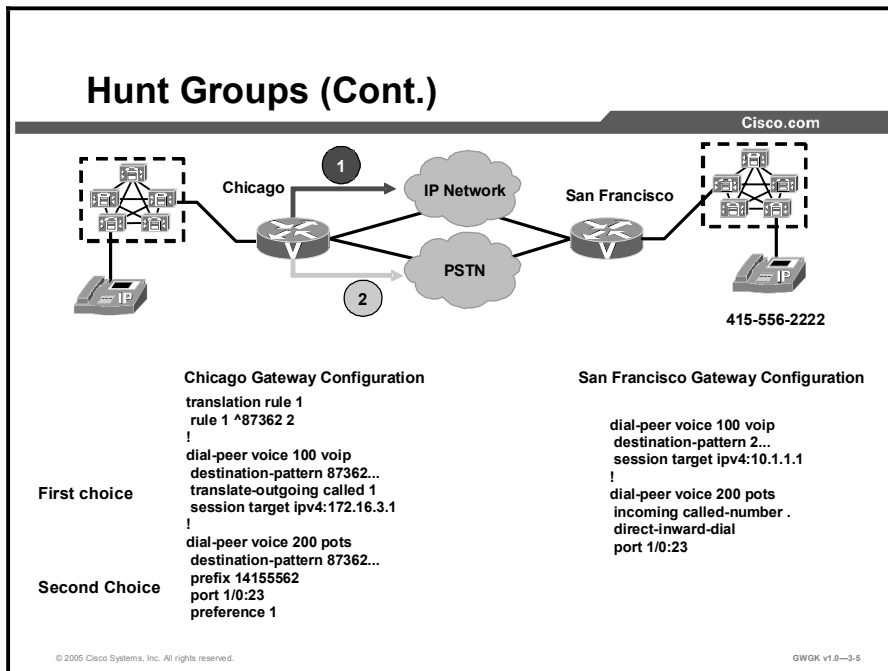
```
dial-peer voice 9 pots
destination pattern 9T
port 0/1:23
preference 0

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

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.8-3-4

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.)



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.

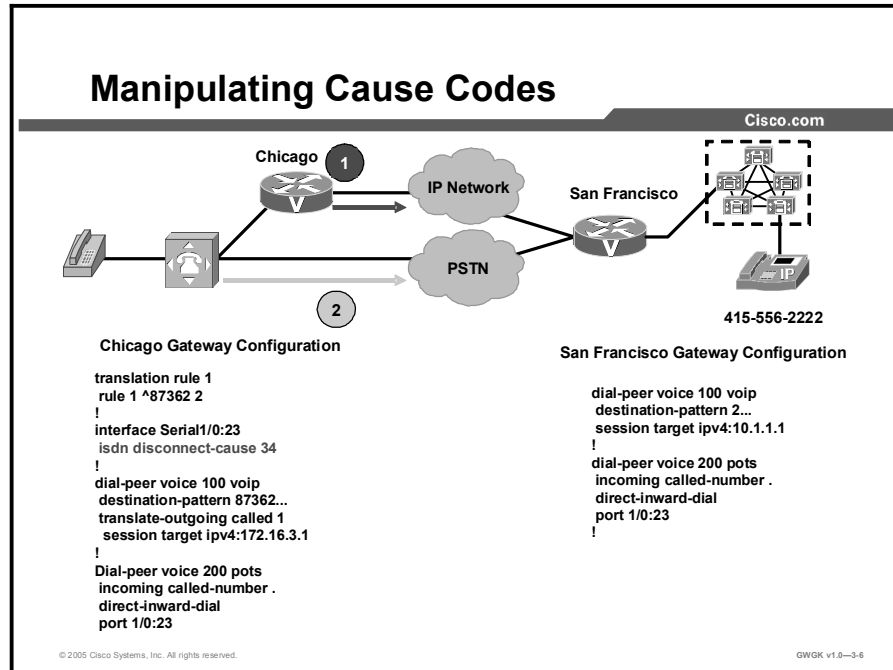
When a call is placed from Chicago to 87362222, dial peer 100 is matched. Because this is a VoIP dial peer, the explicitly matched digits are not stripped. Because the dial peer in the San Francisco gateway will match the extension, a simple translation rule is configured to strip off the access code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



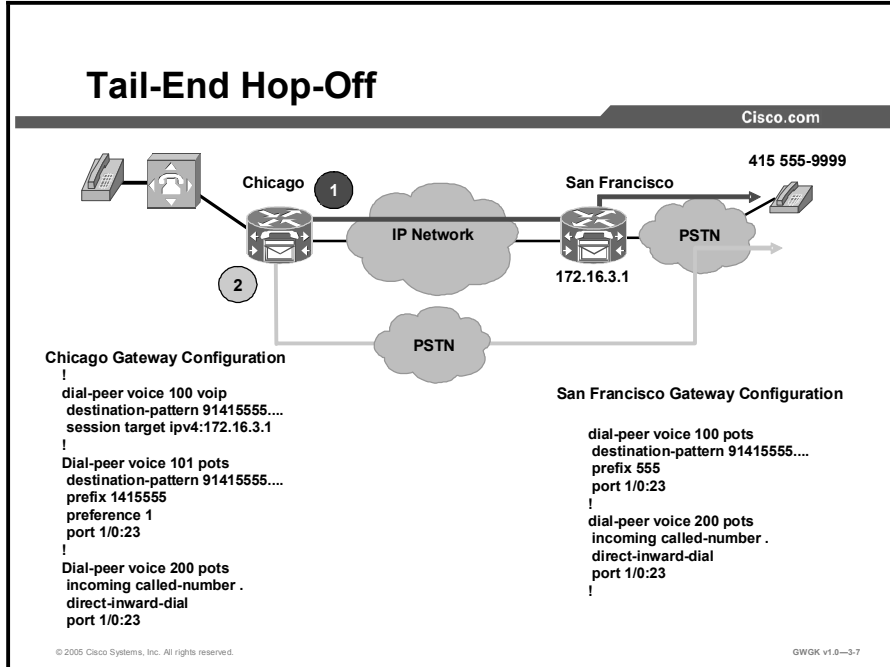
This figure shows a typical PBX toll-bypass integration. In this example, the second route is controlled by the PBX instead of by the gateway. The PBX will determine whether to reroute the call based on the disconnect cause code returned by the gateway. For example, a PBX may not attempt a reroute if 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](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.

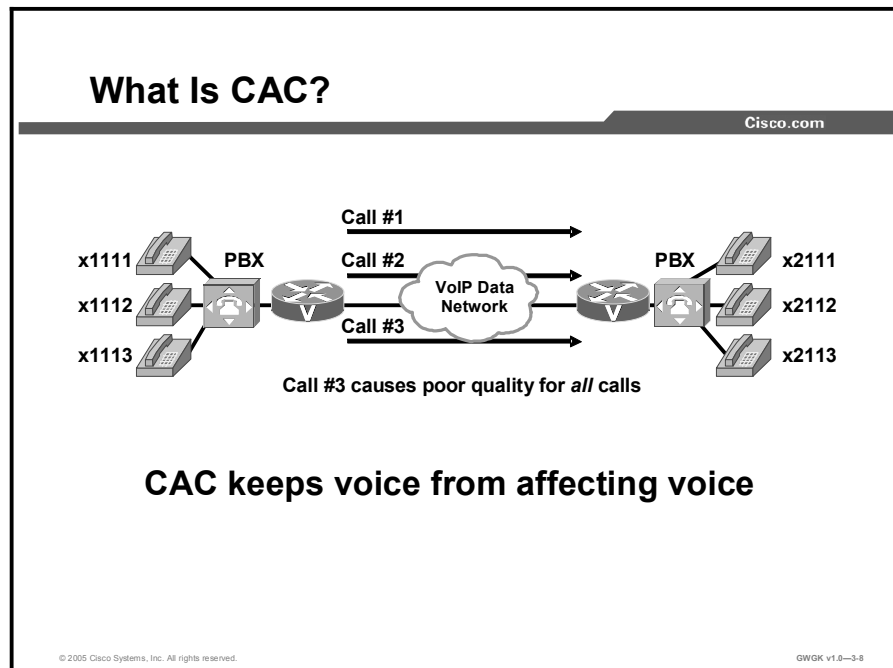


TEHO allows an enterprise to route long-distance calls over the IP WAN to off-net locations. The example in the figure expands on the previous example and show that TEHO allows calls from Chicago to San Francisco to route over the IP WAN as the first choice and over the PSTN as the alternate choice. 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.



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 queuing, 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 queuing 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 queuing 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.

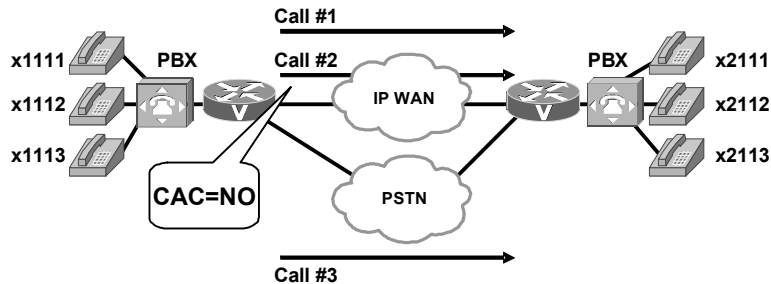
Network congestion cannot be resolved in this manner when real-time traffic, sensitive to both latency and packet loss, is present, without jeopardizing the QoS expected by the users of that traffic. For real-time delay-sensitive traffic such as voice, it is better to deny network access under congestion 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

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK 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

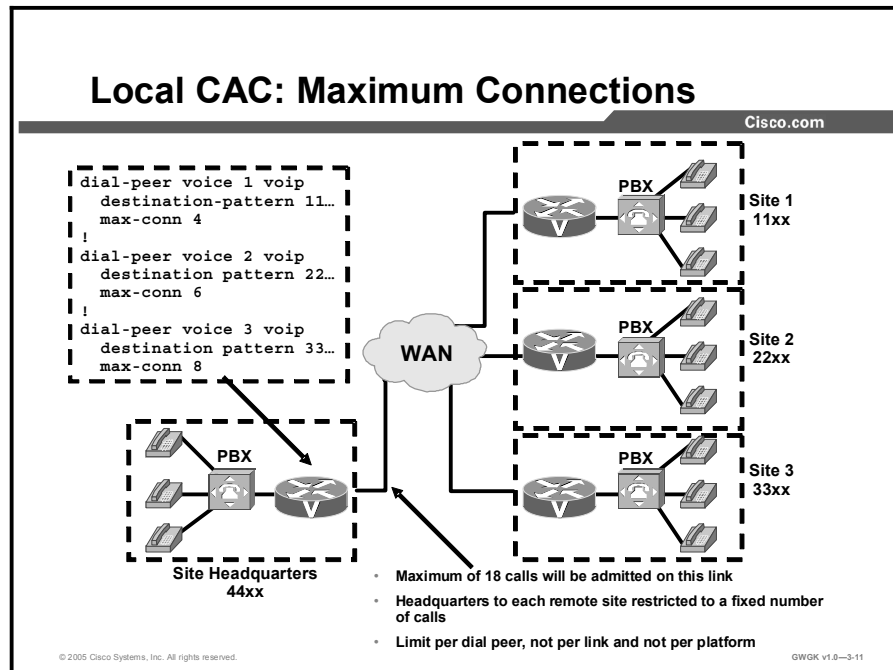
© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-3-10

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.



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**

© 2005 Cisco Systems, Inc. All rights reserved. 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**

© 2005 Cisco Systems, Inc. All rights reserved.

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.

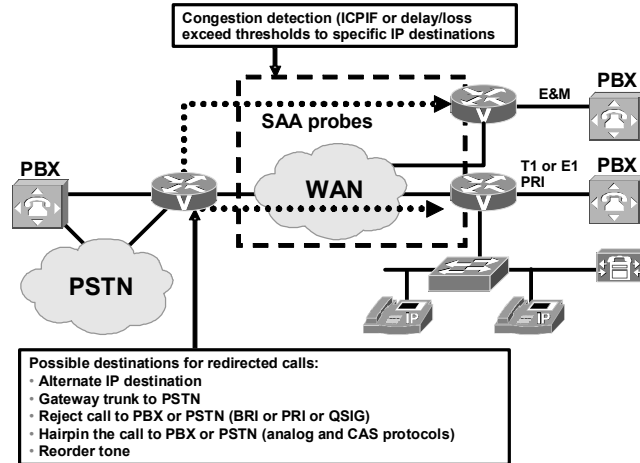
## SAA Protocol

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



© 2005 Cisco Systems, Inc. All rights reserved.

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:

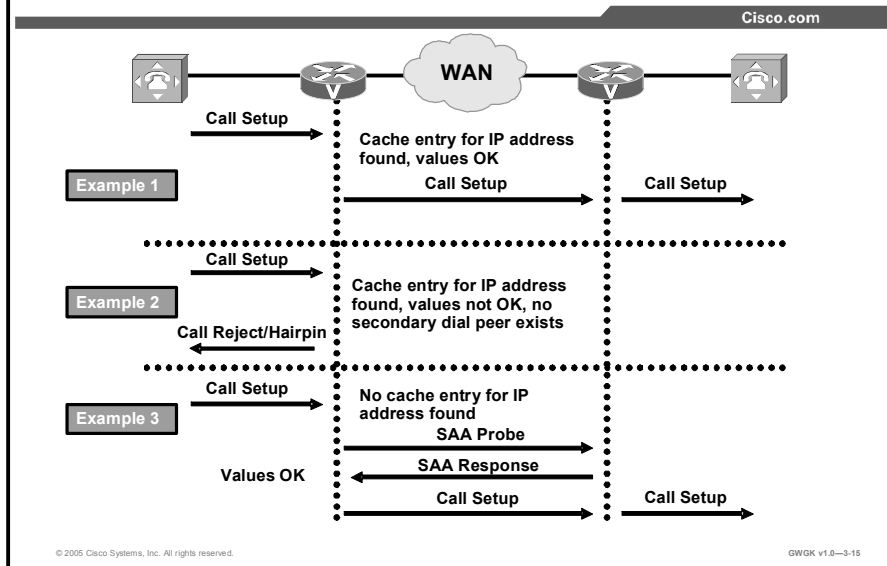
- **5:** Very good
- **10:** Good
- **20:** Adequate
- **30:** Limiting case
- **45:** Exceptional limiting case
- **55:** Customers likely to react strongly

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



### 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

Cisco.com

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—3-16

## 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>call fallback</code>                   | <p>To enable a call request to fall back to a specific dial peer in case of network congestion, use the <b>call fallback</b> command in dial-peer configuration mode. To disable PSTN fallback for a specific dial peer, use the no form of this command.</p> <p>Disabling the <b>call fallback</b> 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.</p>                                                                                                                                                                                                                                                                            |
| <code>call fallback active</code>            | <p>To enable a call request to fall back to alternate dial peers in case of network congestion, use the <b>call fallback active</b> command in global configuration mode. To disable PSTN fallback, use the no form of this command.</p> <p>Enabling the <b>call fallback active</b> command determines whether calls should be accepted or rejected based on the probing of network conditions. The <b>call fallback active</b> 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.</p> <p>Use the <b>call fallback threshold delay loss</b> or <b>call fallback threshold icpif</b> command to set the threshold parameters.</p> |
| <code>call fallback cache-size number</code> | <p>To specify the <b>call fallback cache-size</b> 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.</p> <p>The cache size can be changed only when the <b>call fallback active</b> command is not enabled.</p> <p>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.</p> <p>The following example specifies 120 cache entries:</p> <pre>Router(config)# call fallback cache-size 120</pre>                                                                                                                                                                                                     |

| Command                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>call fallback instantaneous-value- weight weight</pre>          | <p>To configure the call fallback subsystem to take an average from the last two probes registered in the cache for call requests, use the <b>call fallback instantaneous-value-weight</b> command in global configuration mode. To return to the default before the average was calculated, use the no form of this command.</p> <p>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.</p> <p>Use the <b>call fallback instantaneous-value-weight</b> 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.</p> <p>The configured weight applies to the new probe first. If the <b>call fallback instantaneous-value-weight</b> 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.</p> |
| <pre>call fallback jitter- probe num-packets number-of-packets</pre> | <p>To specify the number of packets in a jitter probe used to determine network conditions, use the <b>call fallback jitter-probe num-packets</b> command in global configuration mode. To restore the default number of packets, use the no form of this command.</p> <p>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 <b>call fallback threshold delay loss</b> or <b>call fallback threshold icpif</b> commands to set the threshold parameters.</p> <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <pre>call fallback jitter- probe precedence precedence-value</pre>   | <p>To specify the priority of the jitter-probe transmission, use the <b>call fallback jitter-probe precedence</b> command in global configuration mode. To restore the default priority, use the no form of this command.</p> <p>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.</p> <p>Use the <b>call fallback jitter-probe precedence</b> command if there are different queuing mechanisms in your network. Enabling the <b>call fallback jitter-probe precedence</b> command sets the precedence for jitter probes to pass through your network.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Command                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>call fallback reject- cause-code number</pre>                    | <p>To enable a specific call fallback reject cause code in case of network congestion, use the <b>call fallback reject-cause-code</b> command in global configuration mode. To reset the code to the default of 49, use the no form of this command.</p> <p>It may be necessary to set the reject cause code to a value that will allow the call processing system to reroute the call.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <pre>call fallback threshold delay delay- value loss loss-value</pre> | <p>To specify the call fallback threshold to use only packet delay and loss values, use the <b>call fallback threshold delay loss</b> command in global configuration mode. To restore the default value, use the no form of this command.</p> <p>Use the <b>call fallback threshold delay loss</b> 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.</p> <p>The amount of delay set by the <b>call fallback threshold delay loss</b> command should not be more than half the amount of the time-to-wait value set by the <b>call fallback wait-timeout</b> command; otherwise, the threshold delay will not work correctly. Because the default value of the <b>call fallback wait-timeout</b> command is set to 300 milliseconds, the user can configure a delay of up to 150 milliseconds for the <b>call fallback threshold delay loss</b> 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 <b>call fallback wait-timeout</b> command.</p>                                                                            |
| <pre>call fallback threshold icpif threshold-value</pre>              | <p>To specify that call fallback use the ICPIF threshold, use the <b>call fallback threshold icpif</b> command in global configuration mode. To restore the default value, use the no form of this command.</p> <p>Use the <b>call fallback threshold icpif</b> 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 <b>call fallback active</b> 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 <b>call fallback monitor</b> command, all calls are connected regardless of the configured threshold or voice quality. In this case, configuring the <b>call fallback threshold icpif</b> command allows you to collect network statistics for further tracking.</p> <p>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.</p> <p>The ICPIF is calculated and used according to the ITU G.113 specification.</p> |

## 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
```

© 2005 Cisco Systems, Inc. All rights reserved.

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                   |                                  |
|-------------------------------------------------|----------------------------------|
| 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-0 and 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 it 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
```

© 2005 Cisco Systems, Inc. All rights reserved.

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 buses 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

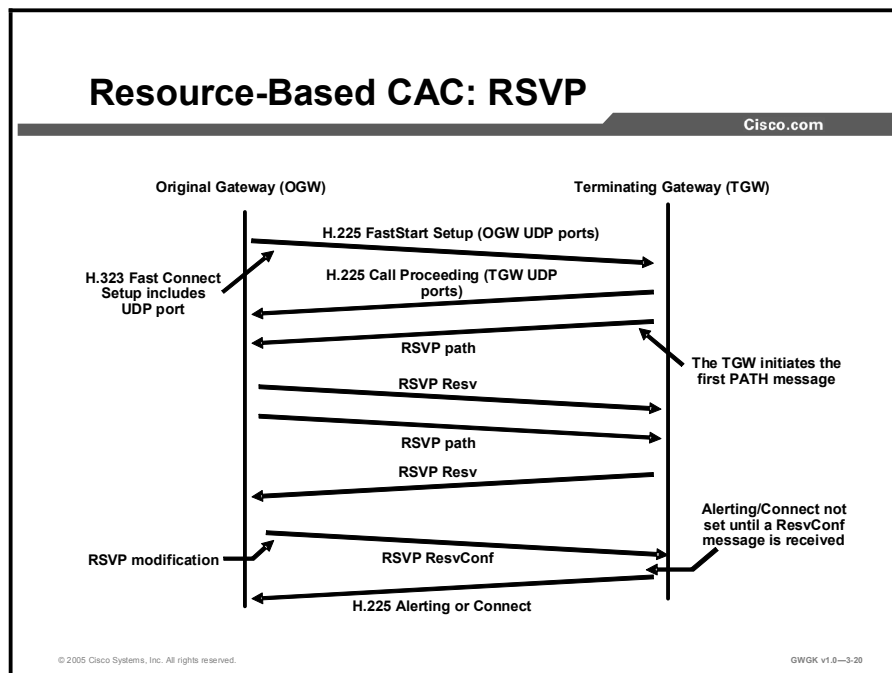
To configure the call treatment, use the following command in global configuration mode:

```
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



### 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

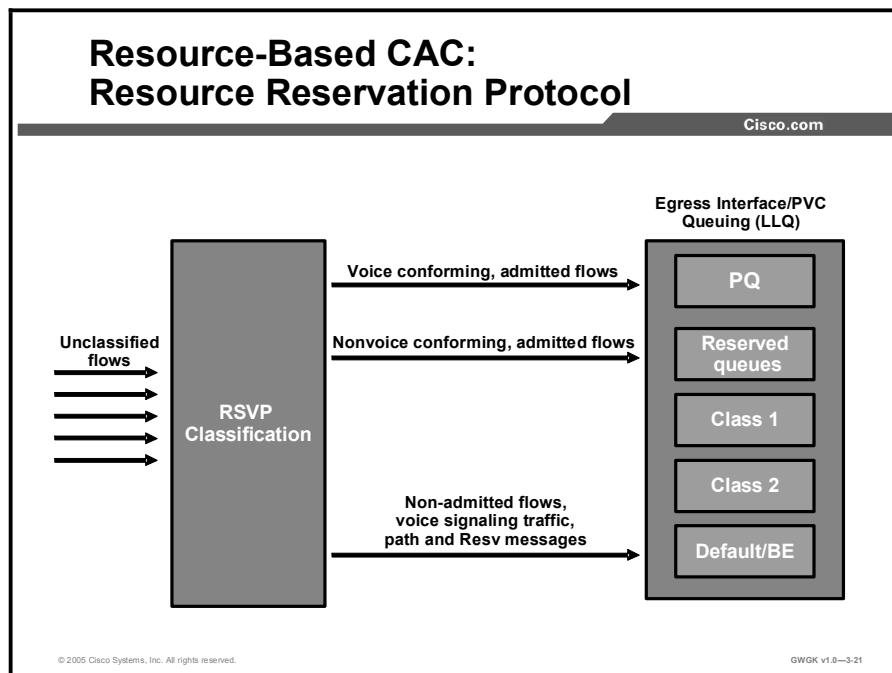
The figure shows a call flow of the H.323 call setup messages and the RSVP reservation messages.

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.



### 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.

© 2005 Cisco Systems, Inc. All rights reserved.

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

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 method.
!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 queuing method.
!Results in LLQ with RSVP.
 frame-relay fair-queue
 frame-relay fragment 160
```

© 2005 Cisco Systems, Inc. All rights reserved.

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.

| <b>Technology Applicability of CAC Mechanisms</b> |            |          |           |                   |             |
|---------------------------------------------------|------------|----------|-----------|-------------------|-------------|
| <small>Cisco.com</small>                          |            |          |           |                   |             |
| 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.

© 2005 Cisco Systems, Inc. All rights reserved. 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

© 2005 Cisco Systems, Inc. All rights reserved.

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.**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-3-27

## References

For additional information, refer to these resources:

- [http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cger/vvfax\\_c/vcltrunk.htm#wp1052598](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cger/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, scalable 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 v1.8—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](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](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](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](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](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](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](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,](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.

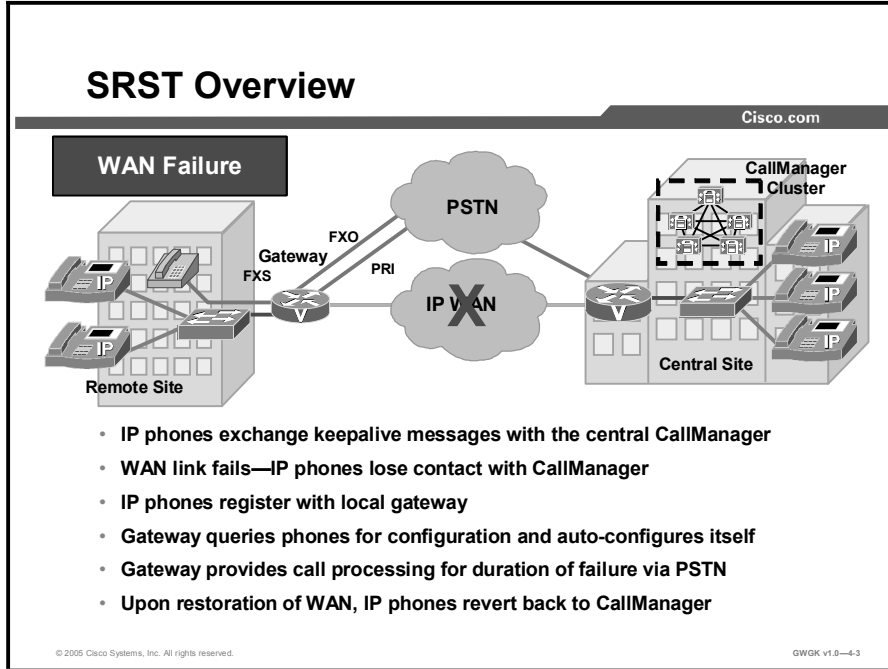
## Objectives

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.

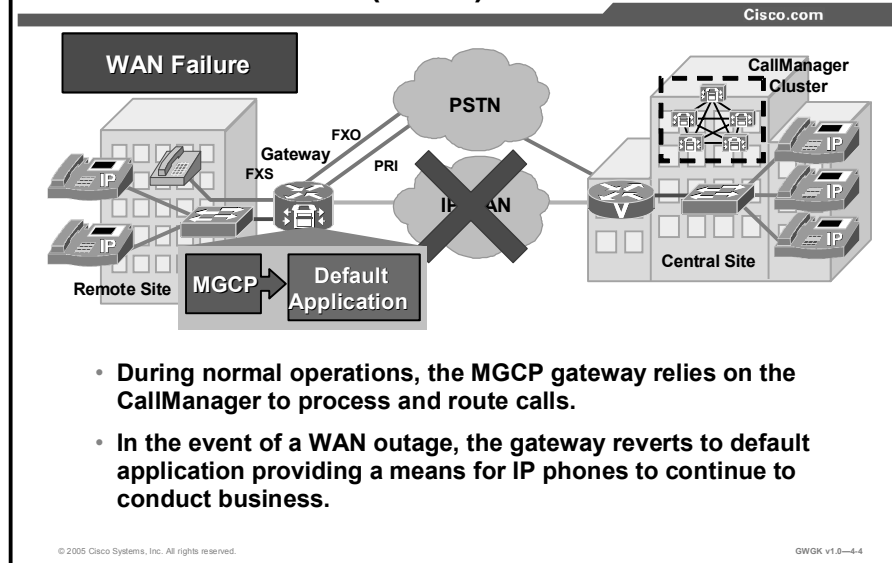


The Cisco SRST software operates by taking advantage of the keepalive packets coming from both the centralized Cisco CallManager cluster and the local IP phones. During normal operations, the Cisco CallManager receives keepalive packets from the IP phones. Cisco CallManager performs call setup, call 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.)



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.

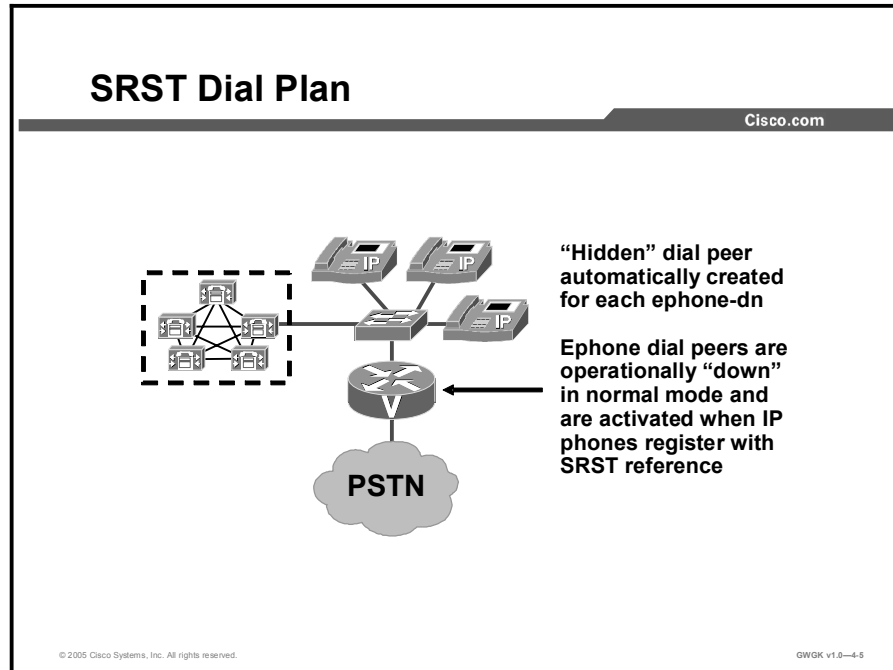
On MGCP gateways, active calls on MGCP channel associated signaling (CAS) or Foreign Exchange Office (FXO) ports will be preserved during a WAN outage. The calls will remain active until either end hangs up the call. IP phones with active calls will not failover to SRST, but rather will stay in a “limbo” 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.



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.)

Cisco.com

```
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

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-4.6

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

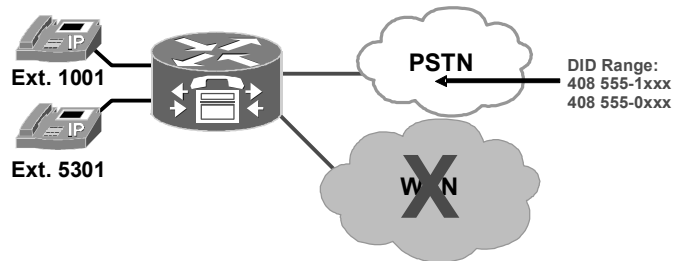
```

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...
```



© 2005 Cisco Systems, Inc. All rights reserved.

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

© 2005 Cisco Systems, Inc. All rights reserved. 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](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](http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_feature_guide09186a008018912f.html)

## Configuring SRST: Enable SRST on the Gateway

Cisco.com

### 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

© 2005 Cisco Systems, Inc. All rights reserved.

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.)

The screenshot displays two overlapping windows from the Cisco CallManager Administration interface. The top window is titled "SRST Reference Configuration" and shows the configuration for a reference named "Remote\_Site\_Chicago-GW". The fields are filled with: IP Address: 172.16.201.1, Port: 5000, and SRST Certificate Provider Port: 2445. The bottom window is titled "Device Pool Configuration" for "Device\_Pool\_Remote\_Cluster". The "SRST Reference" field is set to "Remote\_Site\_Chicago-GW".

**SRST Reference Configuration**

SRST Reference: Remote\_Site\_Chicago-GW  
Status: Update completed

Copy Update Delete Reset Devices

SRST Reference Name\* Remote\_Site\_Chicago-GW

IP Address\* 172.16.201.1

Port\* 5000

Is SRST Secure?

SRST Certificate Provider Port\* 2445

\* indicates required item

**Device Pool Configuration**

Device Pool: Device\_Pool\_Remote\_Cluster (1 members:\*)

Status: Ready

Copy Update Delete Reset Devices

**Device Pool Settings**

Device Pool Name Device\_Pool\_Remote\_Cluster

Cisco CallManager Group\* CM\_A\_B

Date/Time Group\* CM\_Local

Region\* Remote\_Cluster

SRSTkey Template\* ServiceUser

SRST Reference\* Remote\_Site\_Chicago-GW

Calling Search Space for Auto-registration\* <None>

Media Resource Group List: <None>

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
```

© 2005 Cisco Systems, Inc. All rights reserved.

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

Cisco.com

### 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.**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-4-12

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](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00802d1c31.html#wp1046574)

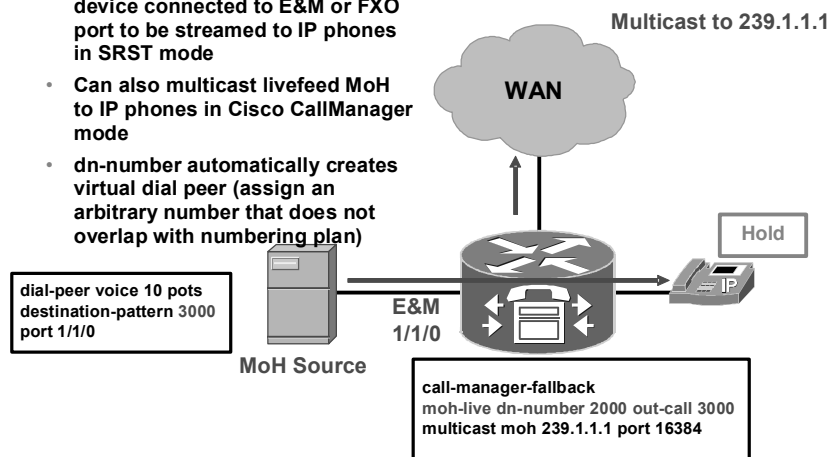
No multicast MOH routing configuration is required for Cisco SRST gateways because each SRST gateway is configured to act as a host running an application that streams multicast MOH packets from the network. The **multicast moh** command declares the Cisco CallManager multicast MOH address and port number 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](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)



© 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.

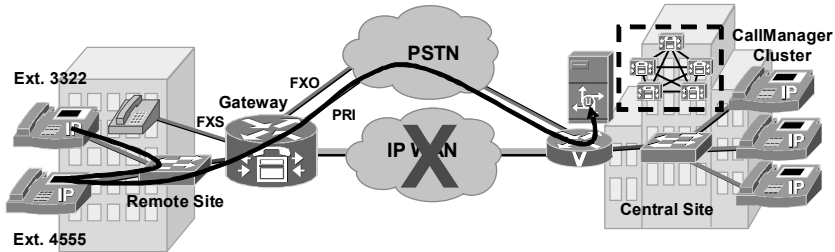
**Step 2** In the Performance window, click the + (plus) icon located at the top of the right pane.

**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.

© 2005 Cisco Systems, Inc. All rights reserved.

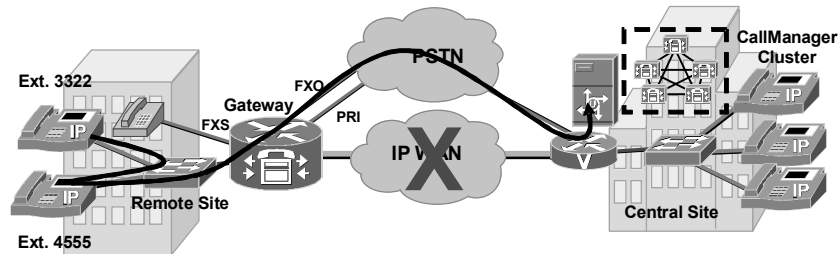
GWGK v1.0-4-14

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.

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK 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](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.   | <pre>vm-integration</pre> <p>Example:</p> <pre>Router(config)# vm-integration</pre>                                                                                                                                      | Enters voice-mail integration mode and enables voice-mail integration with DTMF and analog voice-mail systems.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 2.   | <pre>pattern direct tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p>Example:</p> <pre>Router(config-vm-int)# pattern direct 2 CGN *</pre>                                   | <p>Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when the user presses the messages button on the phone.</p> <ul style="list-style-type: none"> <li>■ <i>tag1</i>—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.</li> <li>■ <i>tag2</i> and <i>tag3</i>—(Optional) See <i>tag1</i>.</li> <li>■ <i>last-tag</i>—See <i>tag1</i>. This tag indicates the end of the pattern.</li> <li>■ <b>CGN</b>—Calling number (CGN) information is sent to the voice-mail system.</li> <li>■ <b>CDN</b>—Called number (CDN) information is sent to the voice-mail system.</li> <li>■ <b>FDN</b>—Forwarding number (FDN) information is sent to the voice-mail system.</li> </ul> |
| 3.   | <pre>pattern ext-to-ext busy tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p>Example:</p> <pre>Router(config-vm-int)# pattern ext-to-ext busy 7 FDN * CGN *</pre>           | 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 <a href="#">Step 2</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 4.   | <pre>pattern ext-to-ext no-answer tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p>Example:</p> <pre>Router(config-vm-int)# pattern ext-to-ext no-answer 5 FDN * CGN *</pre> | 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 <a href="#">Step 2</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Step | Command Action                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.   | <pre>pattern trunk-to-ext busy tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p>Example:</p> <pre>Router(config-vm-int)# pattern trunk-to-ext busy 6 FDN * CGN *</pre>           | <p>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 <a href="#">Step 2</a>.</p>        |
| 6.   | <pre>pattern trunk-to-ext no-answer tag1 {CGN   CDN   FDN} [tag2 {CGN   CDN   FDN}] [tag3 {CGN   CDN   FDN}] [last-tag]</pre> <p>Example:</p> <pre>Router(config-vm-int)# pattern trunk-to-ext no-answer 4 FDN * CGN *</pre> | <p>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 <a href="#">Step 2</a>.</p> |

## 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.**

© 2005 Cisco Systems, Inc. All rights reserved.

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](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b4f.html).

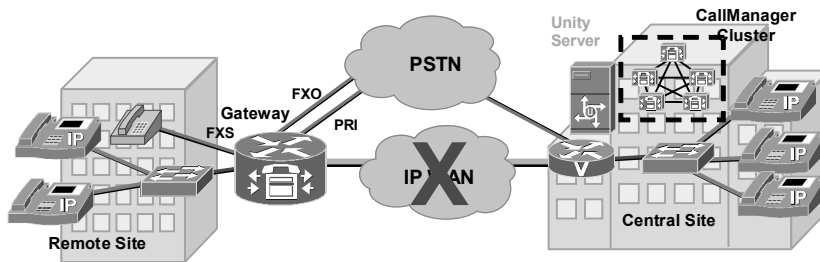
For information on call routing instructions using DTMF digit patterns, go to [http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products\\_administration\\_guide\\_chapter09186a00802a01f8.html#wp1363986](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_administration_guide_chapter09186a00802a01f8.html#wp1363986).

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](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](http://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.

© 2005 Cisco Systems, Inc. All rights reserved.

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 user 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

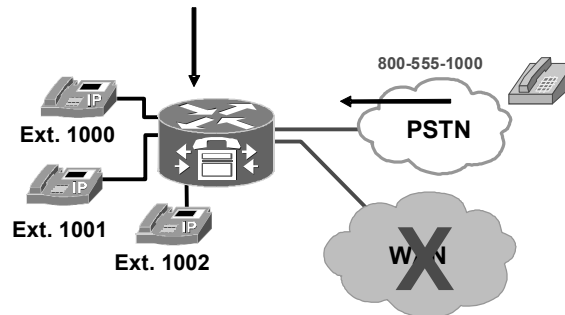
 dial-peer voice 4 pots
 application srst-aa
 destination-pattern 9T
 incoming called-number 1010
 direct-inward-dial
 preference 1
 port 0/1/0:23
 forward-digits all
```



## 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
```



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-4-18

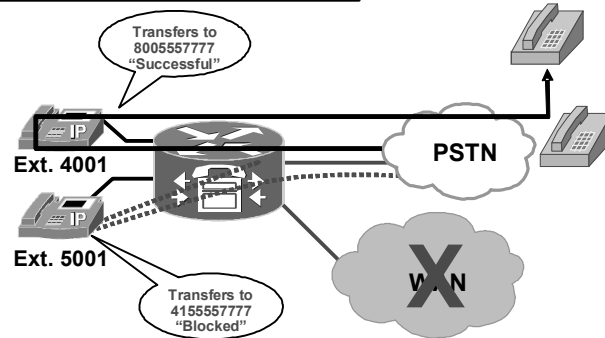
This figure shows an 800 number terminating at the SRST site. The dial peer on the gateway has an incoming called number that matches the number defined in the **pickup** command. In this figure, an incoming call to 8005551000 will ring numbers 1000 through 1002 randomly. Extensions 1001 through 1002 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
```



© 2005 Cisco Systems, Inc. All rights reserved.

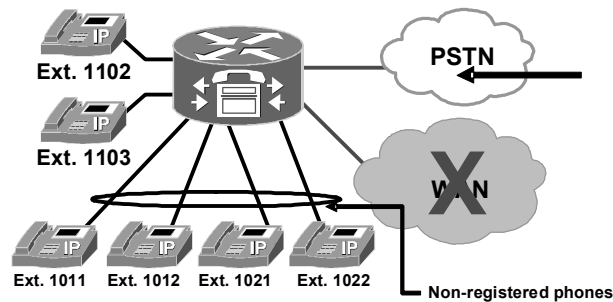
GWGK v1.0-4-19

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 DN's per Phone

Cisco.com

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

© 2005 Cisco Systems, Inc. All rights reserved.

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.**

© 2005 Cisco Systems, Inc. All rights reserved.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](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 as 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.

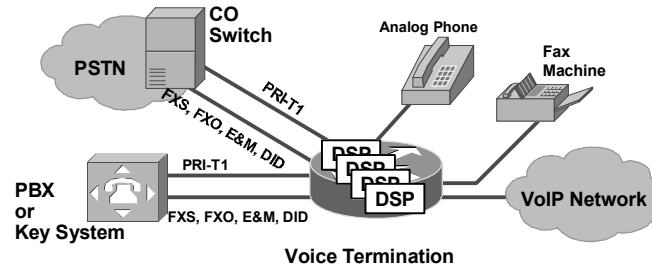
Through the use of DSPs, media termination points extend supplementary services, such as call hold, call transfer, call park, and conferencing that are otherwise not available when a call is routed to an H.323 endpoint. Some H.323 gateways may require that calls use an MTP to enable supplementary call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

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**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-44

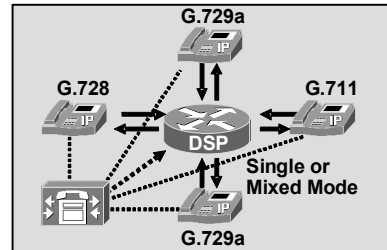
Voice termination applies to a call that has two call legs, one leg on a TDM interface and the second leg on a VoIP connection. The TDM leg must be terminated by hardware that performs coding and decoding as well as packetizing the voice stream. This voice termination function is performed by DSP resources 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



© 2005 Cisco Systems, Inc. All rights reserved.

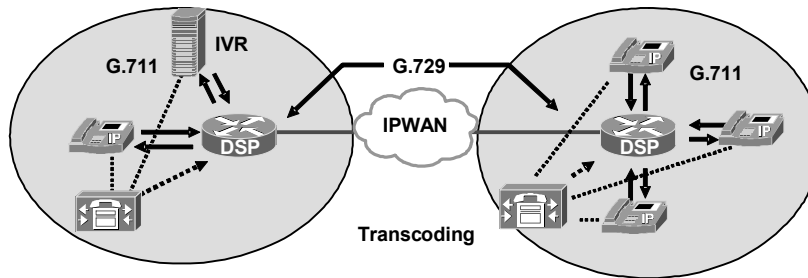
GWGK v1.0-4-5

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 another
- 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



© 2005 Cisco Systems, Inc. All rights reserved.

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.)

Cisco.com

- **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 invoked.**
- **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.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—4.7

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 than 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 the same.

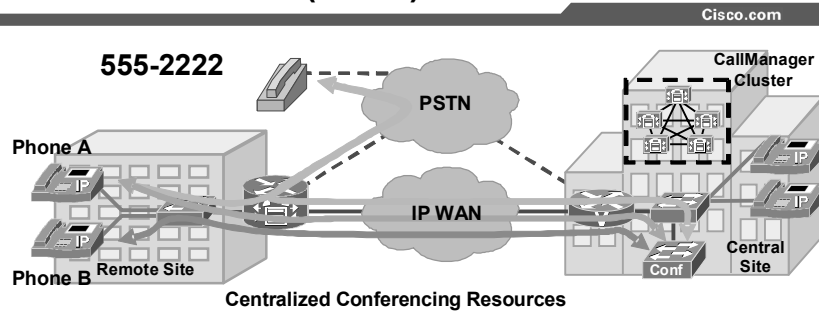
Software MTP specifications are described here:

- 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.)



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

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-4.8

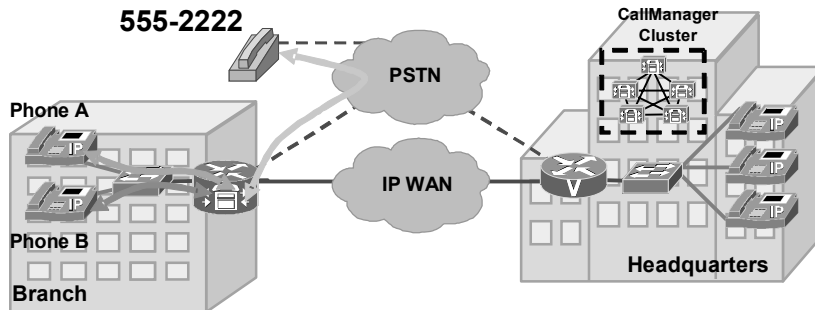
When there are no DSP resources at the remote site, bandwidth use over the IP WAN can become an issue. This figure discusses some issues relative to hosting conferencing at the central site as opposed to deploying DSP resources at the remote site.

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.)

Cisco.com



### Distributed Conferencing Resources

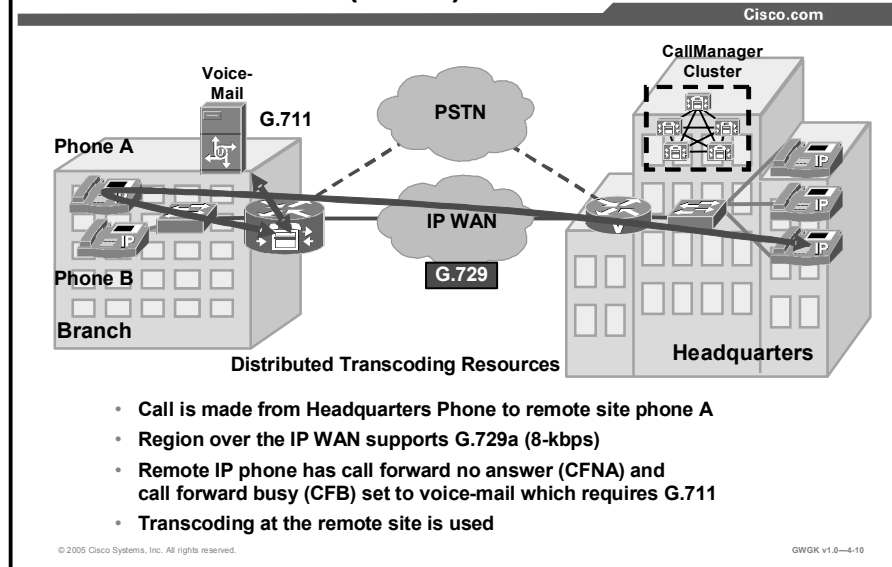
- **Conference between Phone A, Phone B, and 555-2222 using no voice traffic across WAN**
- **Uses DSPs in the branch router**

© 2005 Cisco Systems, Inc. All rights reserved.

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.)



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.**

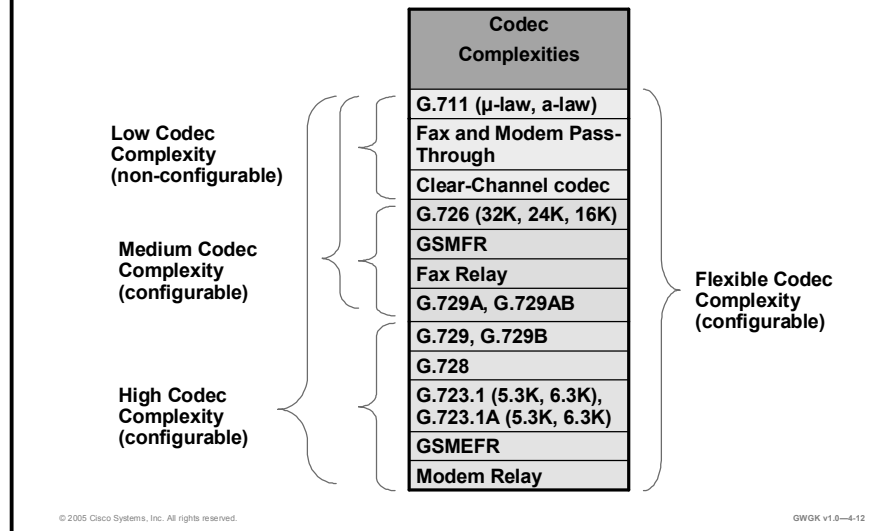
© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0-4-11

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.)

Cisco.com



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 ( $\mu$ -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

© 2005 Cisco Systems, Inc. All rights reserved.

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.)

Cisco.com

- **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.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-4-14

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.)

Cisco.com

- **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
```

© 2005 Cisco Systems, Inc. All rights reserved.

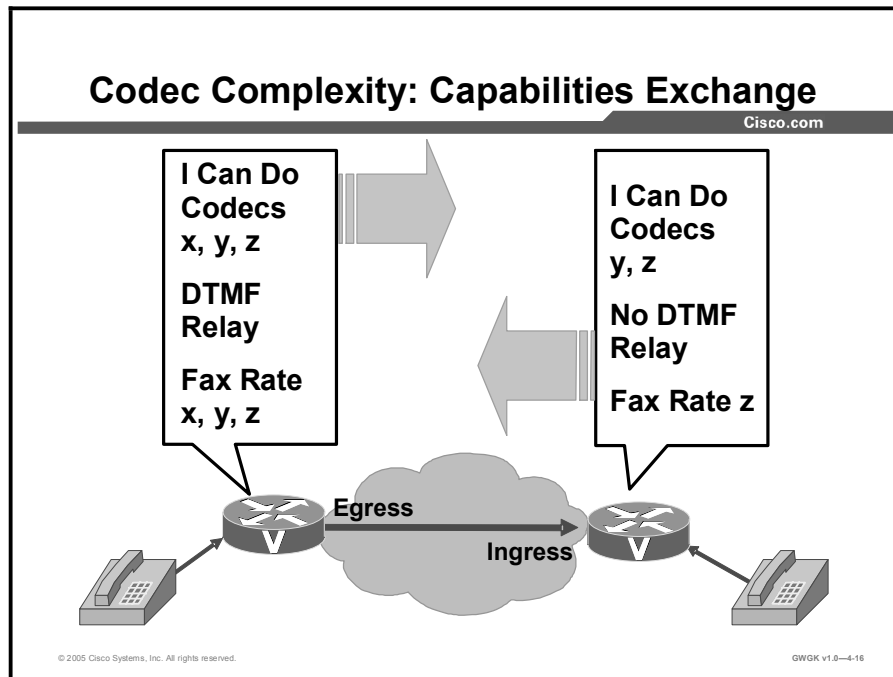
GWGK v1.0-4-15

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.





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)**

© 2005 Cisco Systems, Inc. All rights reserved.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 be 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

The screenshot shows a web browser window titled 'DSP Calculator'. The page has a navigation bar with four tabs: '1. ROUTER AND SOFTWARE VERSIONS', '2. CONFIGURATION', '3. ADVANCED OPTIONS', and '4. RESULTS'. The first tab is active. Below the navigation bar, the heading 'Select Router and Software Versions' is displayed. There are four dropdown menus: 'Router Model' (set to 'Cisco 2821'), 'IOS Mainline Release' (set to 'Select One'), 'IOS T Train Release' (set to '12.3(11)T'), and 'IOS Special Release' (set to 'Select One'). A 'Next' button is located below the 'IOS Special Release' dropdown.

- **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](http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl)

© 2005 Cisco Systems, Inc. All rights reserved.

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 data 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.)

Cisco.com

**DSP Calculator**

1. ROUTER AND SOFTWARE VERSIONS | 2. CONFIGURATION | 3. ADVANCED OPTIONS | 4. RESULTS

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**

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

© 2005 Cisco Systems, Inc. All rights reserved.

- **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**

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

Advanced Option | Submit | Reset

GWGK v1.0-4-21

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 the 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

**DSP Calculator**

1. ROUTER AND SOFTWARE VERSIONS | 2. CONFIGURATION | 3. ADVANCED OPTIONS | 4. RESULTS

**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       | 6                                                | 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**

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.

|                            | Onboard                                                                                                                           | NM1                                                                                                                               | CLI Information          |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Optimized Result (Default) | 7 DSP(s),<br>one PVDM2-48 + one PVDM2-64<br>or<br>one PVDM2-16 + one PVDM2-32 + one PVDM2-64<br>or<br>one PVDM2-16 + two PVDM2-48 | 7 DSP(s),<br>one PVDM2-48 + one PVDM2-64<br>or<br>one PVDM2-16 + one PVDM2-32 + one PVDM2-64<br>or<br>one PVDM2-16 + two PVDM2-48 | <a href="#">CLI Info</a> |
| Normal Result              | N/A                                                                                                                               | N/A                                                                                                                               | N/A                      |
| Worst Case Result          | 9 DSP(s),<br>one PVDM2-16 + two PVDM2-64<br>or<br>three PVDM2-48                                                                  | 12 DSP(s),<br>three PVDM2-64<br>or<br>four PVDM2-48                                                                               | <a href="#">CLI Info</a> |

Save Send Mail

- **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

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

```
scdp local <local interface>
scdp ccm <call manager IP address> identifier <ccm ID #> version <version #>
scdp
!
scdp 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
```

© 2005 Cisco Systems, Inc. All rights reserved.

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

Cisco.com

**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 XCD00F23CD6100
 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**

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0—4-25

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:

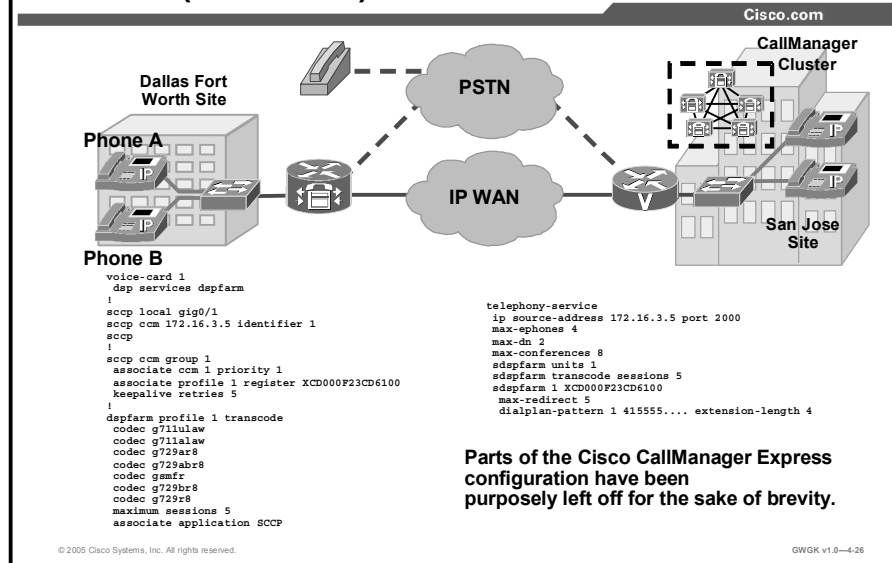
- Step 1**    **enable**
- Step 2**    **configure terminal**
- Step 3**    **voice-card *slot***
- Step 4**    **dsp services dspfarm**
- Step 5**    **exit**
- Step 6**    **dspfarm confbridge maximum sessions *number***
- Step 7**    **dspfarm transcoder maximum sessions *number***
- Step 8**    **dspfarm**
- 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)

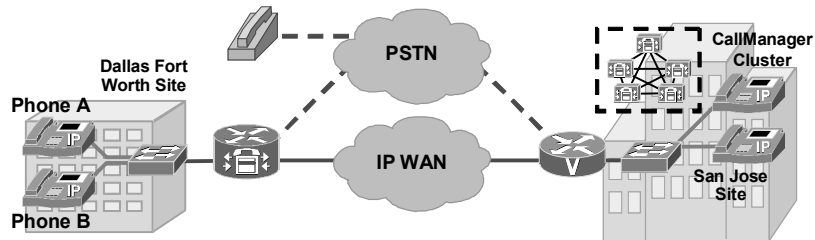


This figure shows the configuration setup for Cisco CallManager Express that has a NM-HVD2. If the gateway used a NM-HDV module the configuration is slightly different.

- **sdpfarm 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.
- **sdpfarm 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.
- **sdpfarm 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)

Cisco.com



```
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
 sdpfarm units 1
 sdpfarm transcode sessions 16
 sdpfarm tag 1 XCD0008E36D65D1
```

© 2005 Cisco Systems, Inc. All rights reserved.

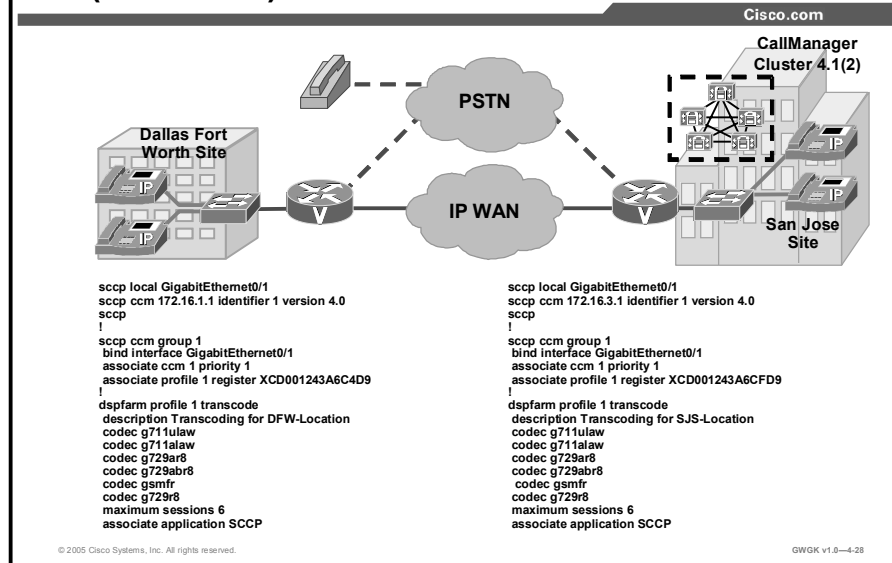
GWGK v1.0-4.27

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)



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

The screenshot displays the Cisco CallManager Administration web interface. The main window is titled "Transcoder Configuration" and shows the configuration for a transcoder. The transcoder is identified as "cod001243A6C4D8" and is registered with Cisco CallManager 172.16.1.1. The device name is also "cod001243A6C4D8" and it belongs to the "Device\_Pool\_AB\_HQ" pool. The transcoder type is "Cisco IOS Enhanced Media Termination Point".

Arrows point from the transcoder ID in the configuration form to the corresponding configuration commands in the adjacent text box. The configuration commands are:

```

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 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)

Cisco.com

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration  
For Cisco IP Telephony Solutions

### 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

```

Add a New Conference Bridge
Meet-Me Number/Pattern Configuration
Cisco
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
codecs g711ulaw
codecs g711alaw
codecs g729ar8
codecs g729abr8
codecs gsmfr
maximum sessions 6
associate application SCCP
!
dspfarm profile 1 conference
codecs g711ulaw
codecs g711alaw
codecs g729ar8
codecs g729abr8
codecs g729br8
codecs g729br8
maximum sessions 4
associate application SCCP

```

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-4-30

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

Cisco.com

- 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 PVDMS2s modules.
- PVDMS is different from PVDMS2. PVDMS are compatible with NM-HDV modules; PVDMS2s 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 PVDMS2.
- 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.

© 2005 Cisco Systems, Inc. All rights reserved.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/calle\\_c/ccm\\_c/intcnf2.htm#wp1052086](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_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/calle\\_c/ccm\\_c/intcnf2.htm#wp1059545](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_c/ccm_c/intcnf2.htm#wp1059545)

Configuring Conferencing and Transcoding (PVDMS-256K):

- [http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/calle\\_c/ccm\\_c/intcnf2.htm#wp1051497](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_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/voicew/ps556/products\\_configuration\\_example09186a0080334294.shtml](http://www.cisco.com/en/US/partner/products/sw/voicew/ps556/products_configuration_example09186a0080334294.shtml)

Cisco DSP Calculator Tool:

- [http://www.cisco.com/cgi-bin/Support/DSP/cisco\\_prodsel.pl](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/comntvoi.htm](http://cco/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/comntvoi.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\\_vfm.htm#wp1049156](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/hdd_vfm.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](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

Cisco.com

**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.**

© 2005 Cisco Systems, Inc. All rights reserved.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 be an actual person or a fax machine.

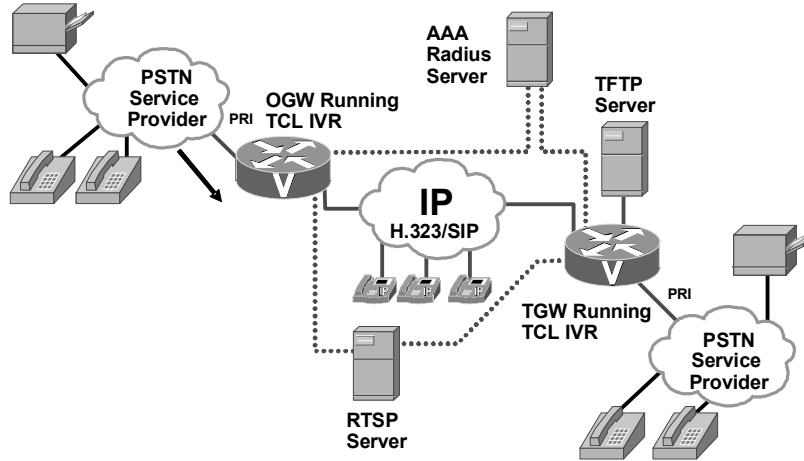
TCL scripts run a routine that launch audio prompts for callers to interact with. These small routines carry out a specific set of instructions, which include the playing out of audio prompts. These audio prompts queue the caller to enter a variety of information such as account numbers, passwords, calling 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 detail 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.)

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

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.

© 2005 Cisco Systems, Inc. All rights reserved.

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

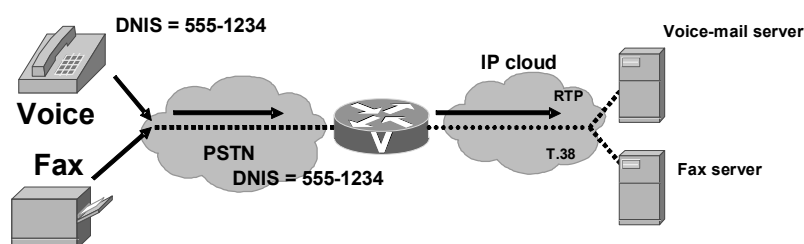
TCL IVR version 1.0 verbs and TCL IVR 2.0 verbs cannot be mixed in a script. You either write a script using version 1.0 verbs in application program interface (API) or using version 2.0 verbs in API.

- 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.
- DTMF 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.

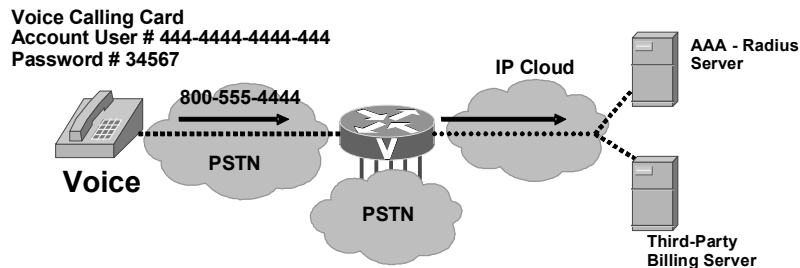
After the application decides whether the call is voice or fax, the call is routed based on the type of call and the dialed number. The gateway uses configuration constructs called dial peers to perform the routing. At its most basic level, the fax detection application makes use of two outgoing dial 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



© 2005 Cisco Systems, Inc. All rights reserved.

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:

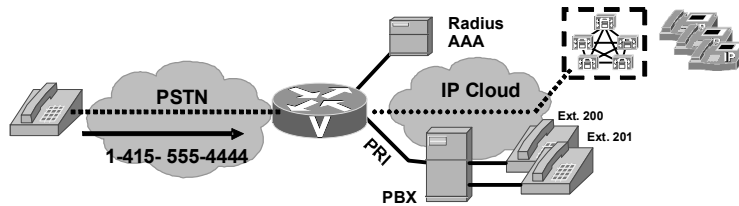
1. A customer calls the access number of the ITSP The application begins with a welcome message
2. The customer is prompted to select a preferred language
3. The customer is prompted for an account number.
4. The prompt returns the amount of credit available on the customer account.
5. The next prompt 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



© 2005 Cisco Systems, Inc. All rights reserved.

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)**

© 2005 Cisco Systems, Inc. All rights reserved.

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_Utone_default-fax.au    | AU Format Sound |
| en_Utone_default-voice.au  | AU Format Sound |
| en_Utone_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.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-4-11

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.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—4-12

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.**

© 2005 Cisco Systems, Inc. All rights reserved.

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

Cisco.com

```
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**

© 2005 Cisco Systems, Inc. All rights reserved.

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.   | <code>Router(config)# call application voice name url</code> | <p>Defines the name of the application to be used with your TCL IVR script. The <i>url</i> argument specifies the location of the file and the access protocol. An example is as follows:</p> <ul style="list-style-type: none"><li>■ flash:scripts/session.tcl</li><li>■ tftp://dirt/sarvi/scripts/session.tcl</li><li>■ ftp://sarvi-ultra/scripts/session.tcl</li><li>■ slot0:scripts/tcl/session..tcl</li></ul> <p><b>Note:</b> You can only configure <i>url</i> if the application named <i>name</i> has not been configured.</p> |

| Step | Command                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.   | <code>Router(config)# call application voice name language digit language</code>                 | Specifies the language used by the audio files. An example is: <code>call application voice test language 1 en</code> . The arguments are as follows: <ul style="list-style-type: none"> <li>■ <i>digit</i>: Specifies 0 through 9.</li> <li>■ <i>language</i>: Specifies two characters that represent a language. For example, "en" for English, "sp" for Spanish, and "ch" for Mandarin. Enter <b>aa</b> to represent all.</li> </ul> |
| 3.   | <code>Router(config)# call application voice name pin-length number</code>                       | Defines the number of characters in the PIN for the designated application. Values are from 0 through 10.                                                                                                                                                                                                                                                                                                                                |
| 4.   | <code>Router(config)# call application voice name retry-count number</code>                      | Defines the number of times a caller is permitted to reenter the PIN for the designated application. Values are from 1 through 5.                                                                                                                                                                                                                                                                                                        |
| 5.   | <code>Router(config)# call application voice name uid-length number</code>                       | 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.   | <code>Router(config)# call application voice name set-location language category location</code> | Defines the location, language, and category of the audio files for the designated application. An example is "set-location en 1 ftp://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                                                                                                                                                                                                                                |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>clid_4digits_npw_3_cli.tcl</code>  | 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. | <b>call application voice uid-len</b><br>min = 1, max = 20, default = 10<br><br><b>call application voice pin-len</b><br>min = 0, max = 10, default = 4<br><br><b>call application voice retry-count</b><br>min = 1, max = 5, default = 3 |
| <code>clid_authen_col_npw_cli.tcl</code> | 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.                                                                          | <b>call application voice retry-count</b><br>min = 1, max = 5, default = 3                                                                                                                                                                |
| <code>clid_authen_collect_cli.tcl</code> | 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.                                   | <b>call application voice retry-count</b><br>min = 1, max = 5, default = 3                                                                                                                                                                |

| Script Name                           | Description                                                                                                                                                                                                              | Parameters                                                                 |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <code>clid_col_npw_3_cli.tcl</code>   | 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.                                                        | <b>call application voice retry-count</b><br>min = 1, max = 5, default = 3 |
| <code>clid_col_npw_npw_cli.tcl</code> | 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. | <b>call application voice retry-count</b><br>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

```

© 2005 Cisco Systems, Inc. All rights reserved.

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)# <b>aaa new-model</b>                                                   | (Optional) Enables AAA security and accounting services.                                                                           |
| 2.   | Router(config)# <b>gw-accounting h323</b>                                              | (Optional) Enables gateway-specific H.323 accounting.                                                                              |
| 3.   | Router(config)# <b>aaa authentication login h323 radius</b>                            | (Optional) Defines a method list called H.323 where RADIUS is defined as the only method of login authentication.                  |
| 4.   | Router(config)# <b>aaa accounting connection h323 start-stop radius</b>                | (Optional) Defines a method list called H.323 where RADIUS is used to perform connection accounting, providing start-stop records. |
| 5.   | Router(config)# <b>radius-server host ip-address auth-port number acct-port number</b> | Identifies the RADIUS server and the ports that will be used for authentication and accounting services.                           |
| 6.   | Router(config)# <b>radius-server key key</b>                                           | Specifies the password used between the gateway and the RADIUS server.                                                             |

| Step | Command                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.   | <code>Router(config)# dial-peer voice<br/>number pots</code>               | Enters dial-peer configuration mode to configure the incoming POTS dial peer. The <i>number</i> argument is a tag that uniquely identifies the dial peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 8.   | <code>Router(dial-peer)# application<br/>name</code>                       | Associates the TCL IVR application with the incoming POTS dial peer. Enter the selected TCL IVR application name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 9.   | <code>Router(config-dial-<br/>peer)# destination-pattern<br/>string</code> | <p>Enters the telephone number associated with this dial peer. The <i>pattern</i> 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:</p> <ul style="list-style-type: none"> <li>■ Plus sign (+): (Optional) Indicates an E.164 standard number. The plus sign (+) is not supported on the Cisco MC3810 multiservice concentrator.</li> <li>■ <i>string</i>: 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: <ul style="list-style-type: none"> <li>— Asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads</li> <li>— Comma (,), which inserts a pause between digits</li> <li>— Period (.), which matches any entered digit (used as a wildcard)</li> </ul> </li> <li>■ T: (Optional) Indicates that the destination-pattern value is a variable length dial-string.</li> </ul> |
| 10.  | <code>Router(config-dial-<br/>peer)# session target</code>                 | 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
hodemst 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](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](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.**

© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.8—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](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](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](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/calle\\_c/ccm\\_c/intcnf2.htm#wp1051497](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_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](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](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](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](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](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/tel\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/tel_c/index.htm).
- *Configuring TCL IVR Applications.*  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax\\_c/vvfivr.pdf](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



# 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.

GWOK 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.

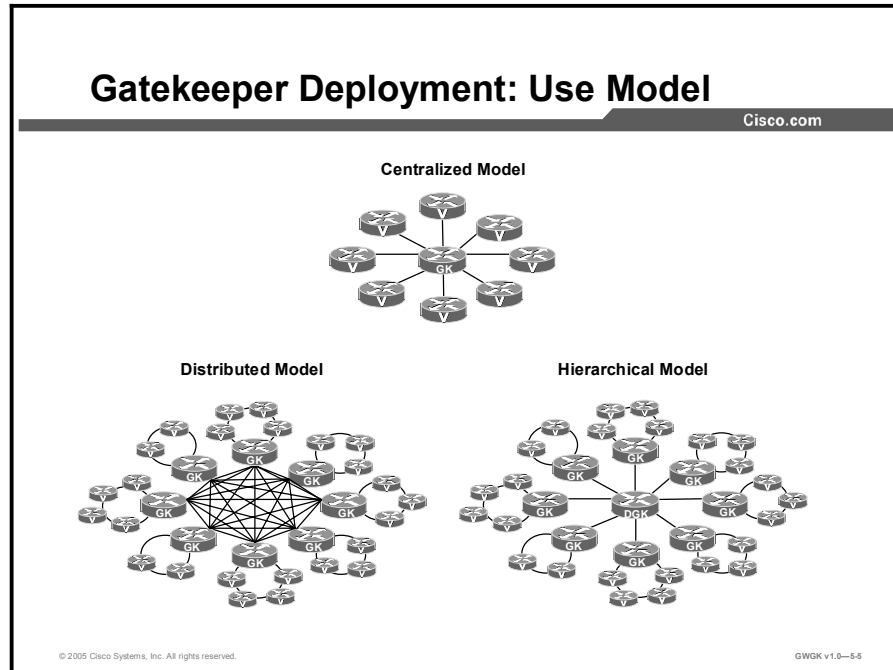
These are just a few of the optional responsibilities the gatekeeper can provide.

- **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.



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

© 2005 Cisco Systems, Inc. All rights reserved. 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 compiled in this figure was derived from the high-performance gatekeeper IOS feature. Here is the IOS feature definition:

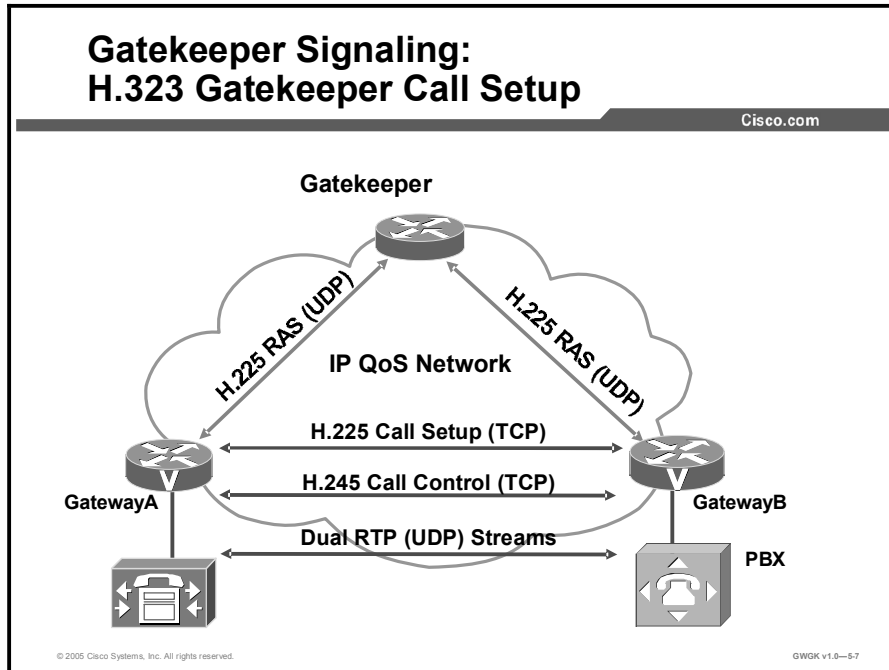
- The high-performance gatekeeper feature introduces new gatekeeper functionality and modifications for facilitating carrier class reliability, security, and performance into the Cisco voice network solution portfolio.
- These H.323 standard-based features have carrier-grade reliability and performance 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](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/ios123/123cgr/vvfax\\_c/callc\\_c/h323\\_c/323config/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax_c/callc_c/h323_c/323config/index.htm)

# Gatekeeper Signaling

This topic describes gatekeeper signaling.



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 choose 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 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)

© 2005 Cisco Systems, Inc. All rights reserved.

GWOK 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.

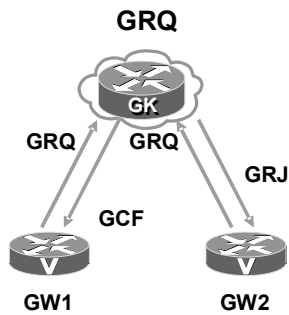
- **Gateway Unregistration Messages:** The unregistration request (URQ) message requests that the association between a terminal and a gatekeeper be broken. Note that the URQ request is bidirectional, that is, a gatekeeper can request a terminal to consider itself unregistered, and a terminal can inform 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

© 2005 Cisco Systems, Inc. All rights reserved.

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.

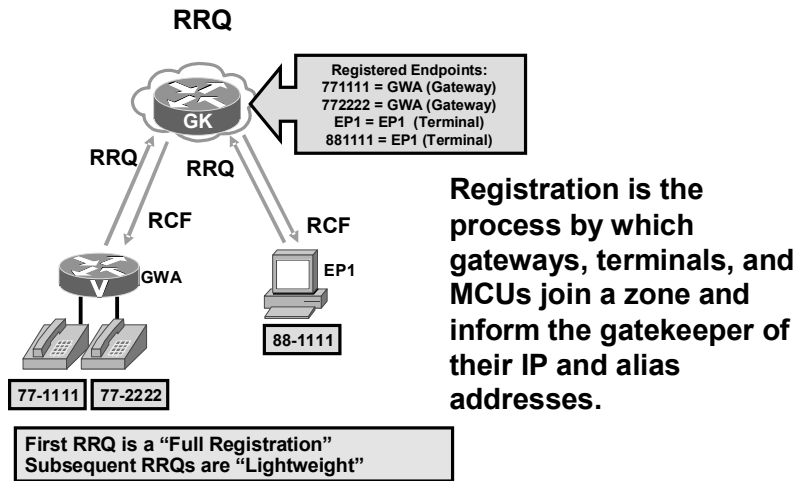
If a gateway requests an explicit gatekeeper name, only that one will respond. If not, the first gatekeeper to respond will become the gatekeeper of that gateway. If a gatekeeper is not available, the gateway will periodically attempt to rediscover. If the gateway discovered gatekeeper has gone off line, 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

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

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.**

© 2005 Cisco Systems, Inc. All rights reserved.

GWK v1.0-511

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.

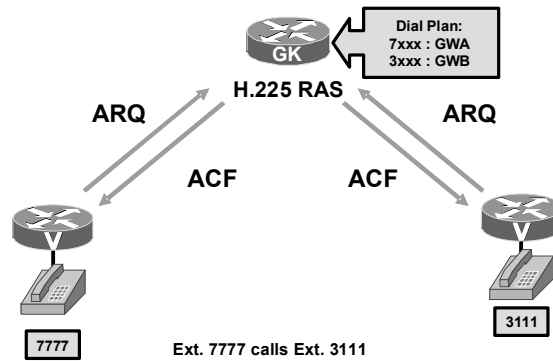
Lightweight registration requires each endpoint to specify a Time to Live (TTL) value in its RRQ message. When a gatekeeper receives an RRQ message with a TTL value, it returns an updated TTL timer value in a RCF message to the endpoint. Shortly before the TTL timer expires, the endpoint sends an RRQ 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



© 2005 Cisco Systems, Inc. All rights reserved.

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:

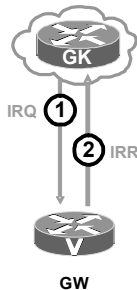
- **calledPartyNotRegistered:** This message is returned because the called party either was never registered or has not renewed its registration with a keepalive RRQ.
- **invalidPermission:** The call violates some proprietary policy within the gatekeeper that is typically set by the administrator of 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.

© 2005 Cisco Systems, Inc. All rights reserved.

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.

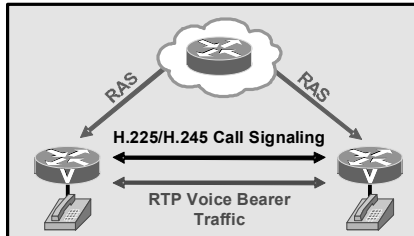


The IRQ message includes the following message:

- **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

Cisco.com



- **Direct Call Signaling**
- **RAS signaling between gateways and gatekeepers**
- **H.225 and H.245 signaling between gateways**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-5-14

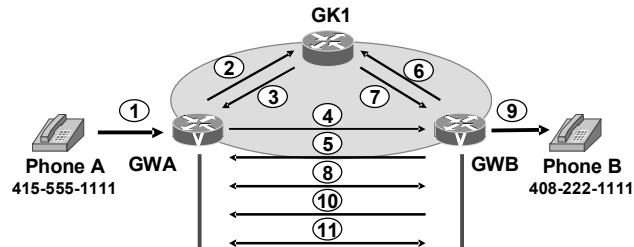
H.225 messages are exchanged between the endpoints if there is no gatekeeper in the H.323 network. When a gatekeeper exists in the network, the H.225 messages are exchanged either directly between the endpoints or between the endpoints after they are routed through the gatekeeper. The two types of direct endpoint signaling are called direct call signaling and gatekeeper-routed call signaling. The gatekeeper decides during RAS admission message exchange which method to choose.

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

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-5-15

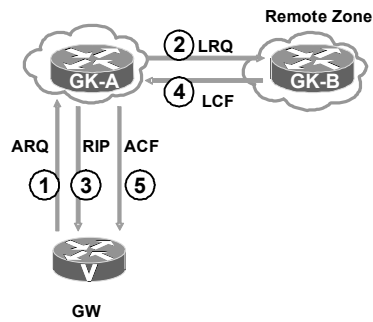
This figure shows the sequence of the signaling events and the basic signaling that takes place between a gateway and gatekeeper. The steps are described in detail here:

- 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.225 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

Cisco.com

### LRQ



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

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0—5-16

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

---

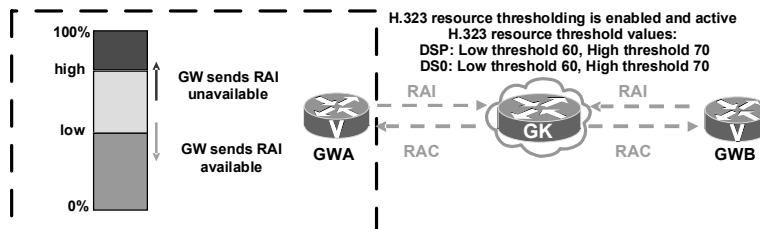
**Note** LRQs are not RAS messages exchanged between gateways and gatekeepers. They are only exchanged between gatekeepers.

---

## Gatekeeper Signaling: Resource Availability Indication

Cisco.com

### RAI



### 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

© 2005 Cisco Systems, Inc. All rights reserved.

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                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>all</b>                   | (Optional) High- and low-parameter settings are applied to all monitored H.323 resources. This is the default condition.                                                                                                                                                                                                                                                                                                                             |
| <b>high percentage-value</b> | (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.                                                                                                                            |
| <b>low percentage-value</b>  | (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  $34 \div 120 = 28\%$ , and the DS-0 utilization is  $34 \div 48 = 70\%$ . 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
```

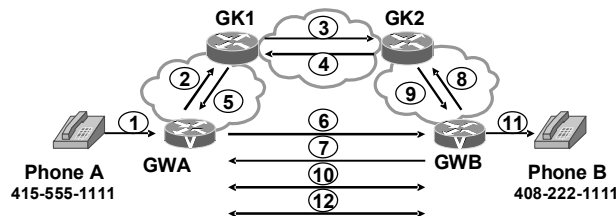
```
Free channels: 14
```



## 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

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-5-18

This figure shows 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.

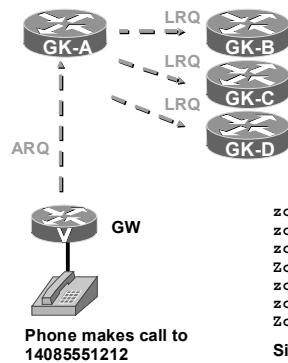
This figure shows the basic gateway to gatekeeper signaling between zones.

- Step 1** Phone A dials the phone number 408-222-1111 for Phone B.
- Step 2** Gateway A sends Gatekeeper1 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

Cisco.com

### 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
```

Simultaneous LRQs sent to remote zone gatekeepers

© 2004 Cisco Systems, Inc. All rights reserved.

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.

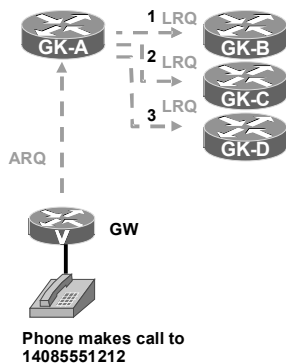
To summarize, Gatekeeper A receives an ARQ from a gateway for 14085551212. Gatekeeper A then blasts LRQs to all gatekeepers, in this case Gatekeeper B, Gatekeeper C, and Gatekeeper D. Gatekeeper A will use the cost and priority values to evaluate the received LCFs to determine where the call should be 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

Cisco.com

### 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



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

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-520

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.

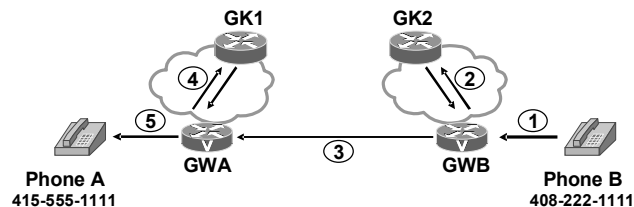
Note that with sequential LRQs, there is a fixed timer between LRQs are sent. Even if Gatekeeper A gets an LRJ back immediately from Gatekeeper B, it will wait a fixed amount of time before sending the next LRQ to Gatekeeper C and Gatekeeper D. You can speed up this process by using the **lrq lrj immediate-advance** 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 GK1
- 5 = GWA signals call disconnect to voice network

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-521

This figure shows basic call disconnect signaling between a gateway and a gatekeeper. The RAS signaling used in this figure 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.com 10.1.1.4 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

The diagram illustrates a hierarchical gatekeeper structure. At the top is a central gatekeeper labeled 'US-GK'. Below it are three regional gatekeepers: 'West' (with prefix 1408\*), 'Central' (with prefix 1312\*), and 'East' (with prefix 1305\*). Each regional gatekeeper is connected to a corresponding PSTN network. A dashed arrow points from the configuration text to the US-GK gatekeeper.

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-5.22

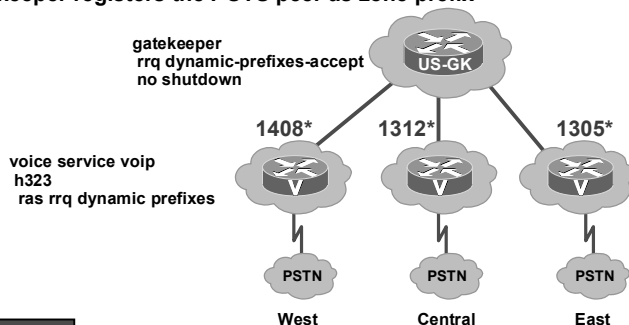
A gatekeeper zone is a collection of endpoints for routing calls. This zone can include H.323 clients, CallManager clusters, or H.323 gateways. This figure shows three regional zones that are managed by one gatekeeper. The gatekeeper US-Gatekeeper manages three major zones: West, Central, and East.

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**



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-523

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                                                                |
|-------------------------------------------------------------|----------------------------------------------------------------------------|
| <code>US-GK (config) # gatekeeper</code>                    | This enters gatekeeper configuration mode                                  |
| <code>US-GK (config-gk) #rrq dynamic-prefixes-accept</code> | This allows US-Gatekeeper to receive the RRQ RAS messages from the gateway |
| <code>US-GK (config-gk) #exit</code>                        | This exits gatekeeper configuration mode                                   |

In the gateway, add these commands to the configuration:

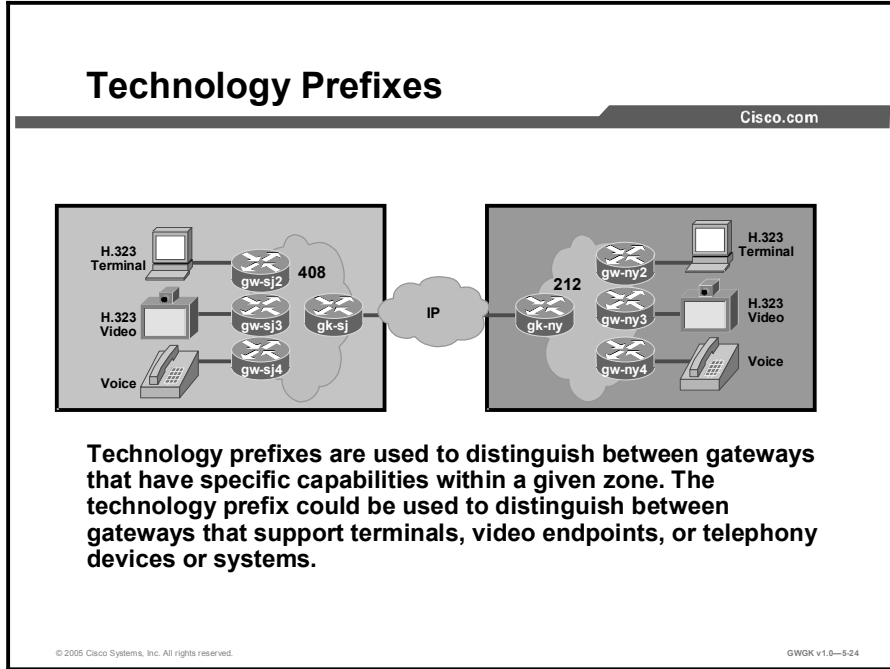
## Gateway Configuration Commands

| Command                                                      | Description                                                                                         |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <code>West (config) #voice service voip</code>               | This enters voice service configuration mode                                                        |
| <code>West (config-voice-serv) #h323</code>                  | This enters the H.323 voice service configuration mode                                              |
| <code>West (conf-serv-h323) #ras rrq dynamic prefixes</code> | This enables the gateway to send and advertisement of dynamic prefixes in additive RRQ RAS messages |
| <code>West (conf-serv-h323) #exit</code>                     | 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.



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:

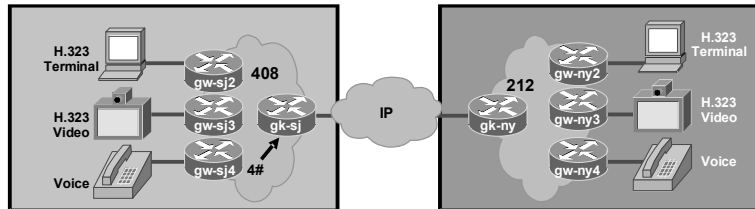
```
gatekeeper
zone local gk-ny cisco.com
zone remote gk-sj cisco.com 172.21.1.48
zone prefix gk-sj 408.....
zone prefix gk-ny 212.....
gw-type-prefix 3# hopoff gk-ny2
gw-type-prefix 4# default-technology
```

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.**

© 2005 Cisco Systems, Inc. All rights reserved.

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.GWOK 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.

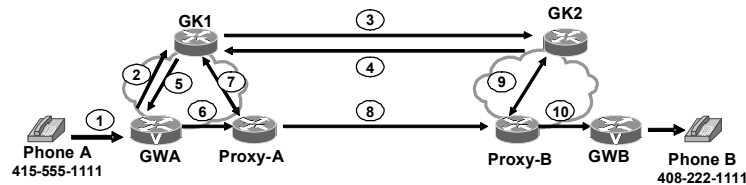
### Proxy Gateway Configuration Example

```
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
- Application-specific routing

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).

## Open API: GKTMP

Cisco.com

The diagram illustrates the GKTMP architecture. At the top is a laptop icon labeled 'Route Server'. Below it is a central cloud containing a router icon labeled 'GK'. Two arrows, one pointing up and one pointing down, connect the Route Server and the GK. Below the GK cloud are two more clouds, each labeled 'PSTN'. Each PSTN cloud is connected to the GK cloud by a dashed line. Each PSTN cloud also contains two router icons labeled 'V'.

- **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

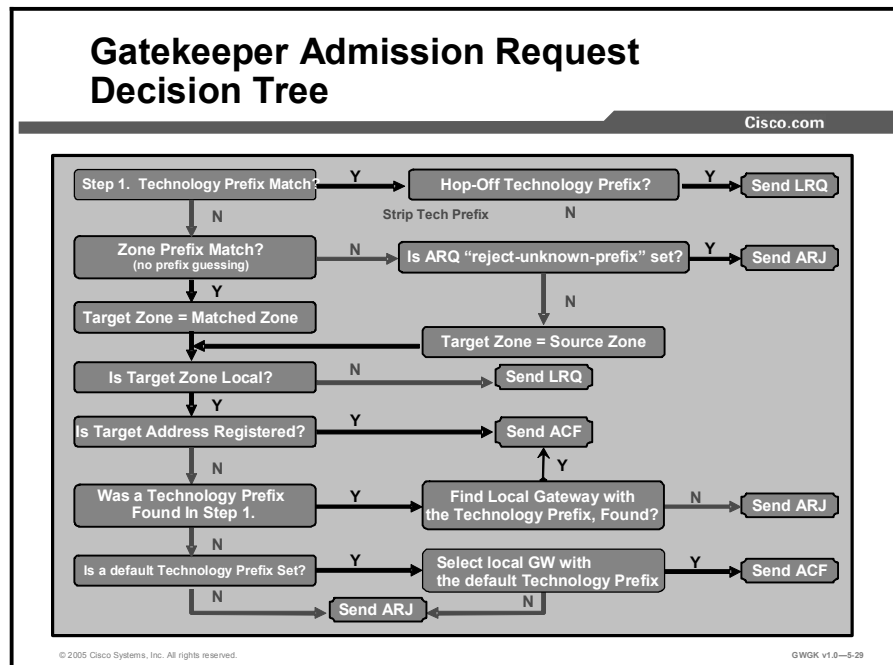
GKTMP can extend the call control intelligence of a gatekeeper by providing an interface to a route application server where advanced routing decisions can be made. It converts incoming RAS messages to text messages and sends them to an off-board server. The server can override default gatekeeper behavior.

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.



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 LQR 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 LQR 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.

© 2005 Cisco Systems, Inc. All rights reserved. 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.

© 2005 Cisco Systems, Inc. All rights reserved. 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 signaled load sharing on large gateway POPs.**

© 2005 Cisco Systems, Inc. All rights reserved.

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](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](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/calle\\_c/h323\\_c/323conf/5gkconf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/calle_c/h323_c/323conf/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.

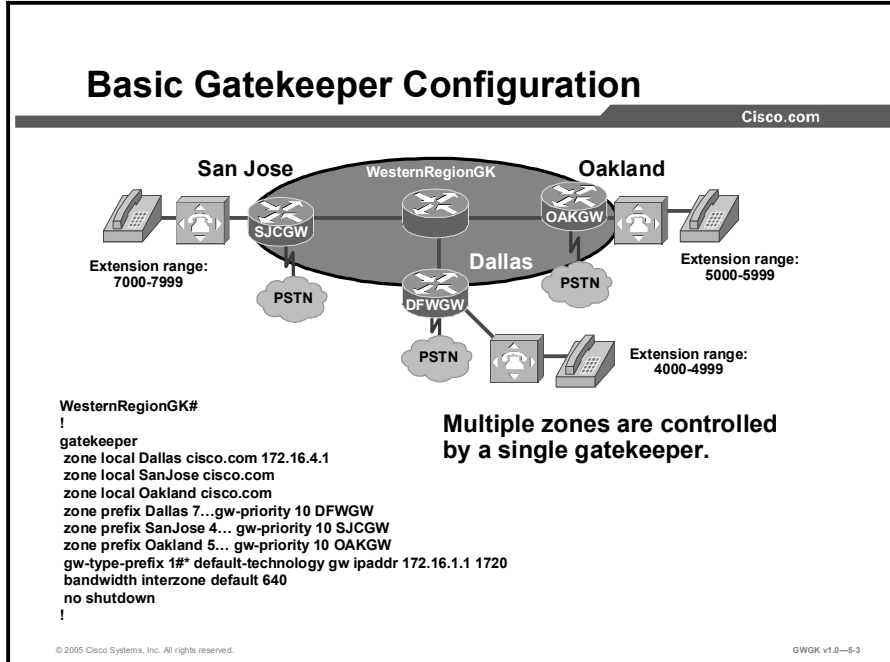
## Objectives

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.

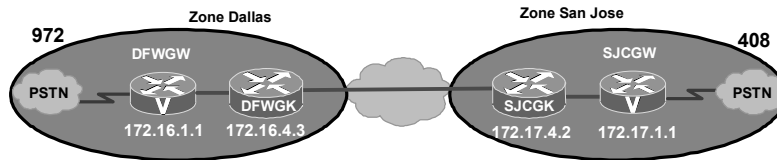


This figure shows a common topology where a gatekeeper, in this scenario Western Region Gatekeeper, manages multiple zones. There can be only one gatekeeper controlling a zone at any time. There are exceptions, however, where backup gatekeepers may be deployed. This topic is covered in the “Configuring Gatekeeper Redundancy” lesson of this module.

## Basic Gatekeeper Configuration (Cont.)

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
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
```

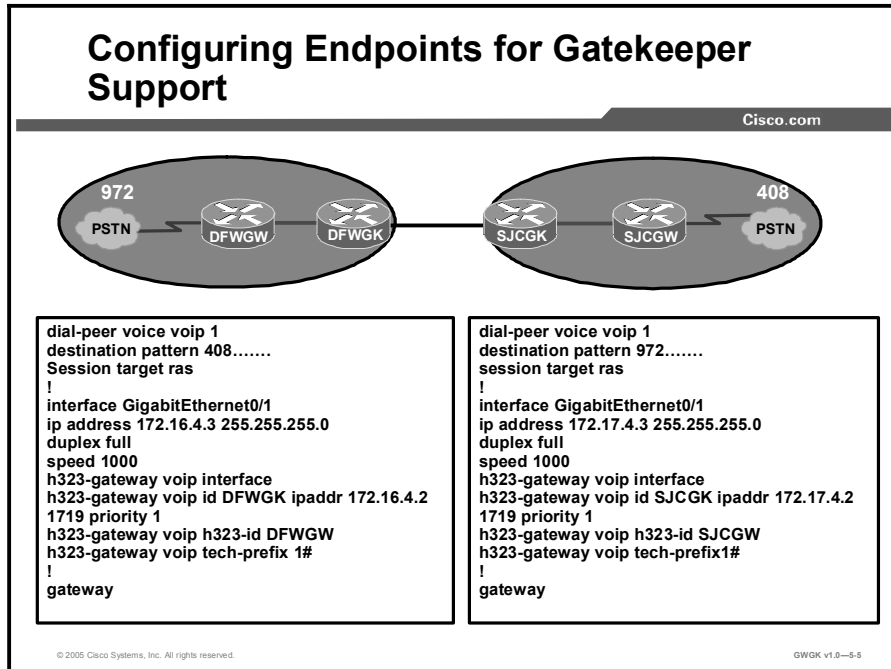
© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-5.4

This figure shows the basic steps in configuring gatekeepers managing local and remote 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.



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.   | <code>gateway</code><br>Example:<br><code>Router(config)# gateway</code>                                            | Enters gateway configuration mode and enables the gateway to register with the gatekeeper |
| 2.   | <code>exit</code><br>Example:<br><code>Router(config-gateway)# exit</code>                                          | Exits the current mode                                                                    |
| 3.   | <code>h323-gateway voip interface</code><br>Example:<br><code>Router(config-if)# h323-gateway voip interface</code> | Identifies this as a VoIP gateway interface                                               |

| Step | Command                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.   | <pre>h323-gateway voip id gatekeeper-id {ipaddr ip- address [port]   multicast} [priority priority]</pre> <p>Example:</p> <pre>Router(config-if)# h323- gateway voip id gk3.gg-dn1 ipaddr 172.18.0.0 1719</pre> | <p>(Optional) Defines the name and location of the gatekeeper for this gateway</p> <p>Keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>■ <i>gatekeeper-id</i>: H.323 identification of the gatekeeper. Must exactly match the gatekeeper ID in the gatekeeper configuration. Recommended format: name.domainname.</li> <li>■ <i>ipaddr ip-address</i>: IP address to be used to identify the gatekeeper.</li> <li>■ <i>port</i>: Port number used.</li> <li>■ <b>multicast</b>: Gateway uses multicast to locate the gatekeeper.</li> <li>■ <b>priority priority</b>: Priority of this gatekeeper. Range: 1 to 127. Default: 127.</li> </ul> |
| 5.   | <pre>h323-gateway voip h323-id interface-id</pre> <p>Example:</p> <pre>Router(config-if)# h323- gateway voip h323-id name@domainname</pre>                                                                      | <p>(Optional) Defines the H.323 name of the gateway, identifying this gateway to its associated gatekeeper</p> <p>Usually this ID is the name of the gateway, with the gatekeeper domain name appended to the end: name@domainname.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 6.   | <pre>h323-gateway voip tech-prefix prefix</pre> <p>Example:</p> <pre>Router(config-if)# h323- gateway voip tech-prefix 2#</pre>                                                                                 | <p>(Optional) Defines the numbers used as the technology prefix that the gateway registers with the gatekeeper</p> <p>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 *.</p>                                                                                                                                                                                                                                                                                                                                                             |
| 7.   | <pre>h323-gateway voip bind srcaddr ip-address</pre> <p>Example:</p> <pre>Router(config-if)# h323- gateway voip bind srcaddr 192.168.0.0</pre>                                                                  | <p>Sets the source IP address to be used for this gateway</p> <p>The argument is as follows:</p> <ul style="list-style-type: none"> <li>■ <i>ip-address</i>: 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.</li> </ul>                                                                                                                                                                                                                                                                                                                                |

## 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

© 2005 Cisco Systems, Inc. All rights reserved. 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

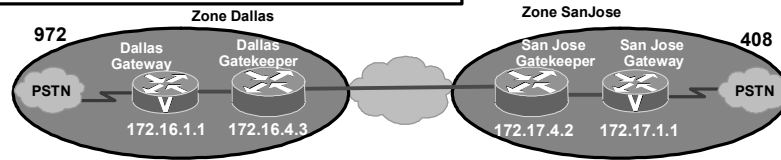


- Multiple logical gatekeepers control the multiple zones on the same Cisco IOS platform.
  - The maximum number of local zones defined in a gatekeeper should not exceed 100.
- **Zone Prefix**
- A gatekeeper can handle more than one zone prefix, but a zone prefix cannot be shared by more than one gatekeeper. 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
```

© 2005 Cisco Systems, Inc. All rights reserved.

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

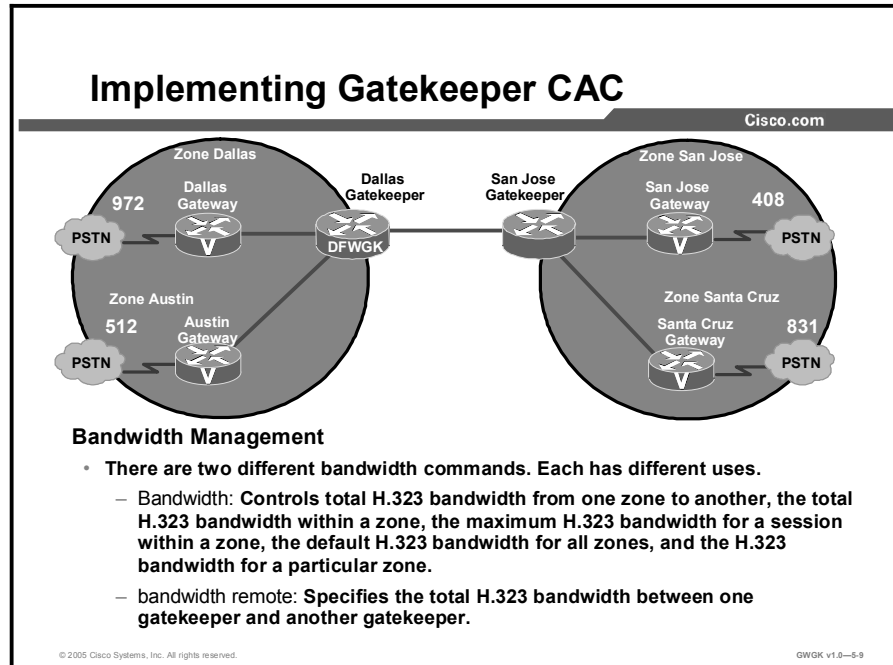
| Step | Command                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Router(config)# <b>gatekeeper</b>                                                                     | Enters gatekeeper configuration mode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 2.   | Router(config-gk)# <b>zone local</b><br><i>gatekeeper-name domain-name</i><br><i>[ras-IP-address]</i> | Specifies a zone controlled by a gatekeeper<br><br>The arguments are as follows: <ul style="list-style-type: none"> <li>■ <i>gatekeeper-name</i>: 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.</li> <li>■ <i>domain-name</i>: Specifies the domain name served by this gatekeeper.</li> <li>■ <i>ras-IP-address</i>: (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.</li> </ul> <p><b>Note:</b> Setting this address for one local zone makes it the address used for all local zones.</p> |

| Step | Command                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.   | <pre>Router(config-gk)# zone prefix gatekeeper-name e164-prefix [blast   seq] [gw-priority priority gw-alias [gw-alias, ...]]</pre> | <p>Adds a prefix to the gatekeeper zone list</p> <p>The keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>■ <i>gatekeeper-name</i>: Specifies the name of a local or remote gatekeeper, which must have been defined by using the <b>zone local</b> or <b>zone remote</b> command.</li> <li>■ <i>e164-prefix</i>: 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.</li> </ul> <p><b>Note:</b> 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.</p> <ul style="list-style-type: none"> <li>■ <i>blast</i>: (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.</li> <li>■ <i>seq</i>: (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.</li> <li>■ <b>gw-priority priority gw-alias</b>: (Optional) Use the <b>gw-priority</b> 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.</li> </ul> <p>Use values from 0 to 10. A 0 value prevents the gatekeeper from using the gateway <i>gw-alias</i> for that prefix. Value 10 places the highest priority on gateway <i>gw-alias</i>. If you do not specify a priority value for a gateway, the value 5 is assigned.</p> <p>To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the pri-0-to-10 value.</p> <p>The <i>gw-alias</i> 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 <b>h323-gateway voip h.323-id</b> command.</p> |

| Step | Command                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.   | <pre>Router(config-gk)# zone subnet local-gatekeeper-name [default   subnet-address {/bits-in- mask   mask-address} enable]</pre> | <p>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.)</p> <p>The keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>■ <i>local-gatekeeper-name</i>: Specifies the name of the local gatekeeper.</li> <li>■ <b>default</b>: (Optional) Applies to all other subnets that are not specifically defined by the <b>zone subnet</b> command.</li> <li>■ <i>subnet-address</i>: (Optional) Specifies the address of the subnet that is being defined.</li> <li>■ <i>bits-in-mask</i>: (Optional) Specifies the number of bits of the mask to be applied to the subnet address.</li> </ul> <p><b>Note:</b> The slash must be entered before this argument.</p> <ul style="list-style-type: none"> <li>■ <i>mask-address</i>: (Optional) Specifies the mask (in dotted string format) to be applied to the subnet address.</li> <li>■ <b>enable</b>: (Optional) Specifies that the gatekeeper accepts discovery and registration from the specified subnets.</li> </ul> <p><b>Note:</b> To define the zone as being all but one set of subnets by disabling that set and enabling all other subnets, use the <b>no</b> form of the command as follows: Configure <b>no zone subnet local-gatekeeper-name subnet-address {/bits-in-mask   mask-address} enable</b>.</p> <p><b>Note:</b> To accept the default behavior, which is that all subnets are enabled, use the <b>no</b> form of the command as follows: <b>no zone subnet local-gatekeeper-name default enable</b>.</p> |
| 5.   | <pre>Router(config-gk)# no shutdown</pre>                                                                                         | Brings the gatekeeper online                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

# Implementing Gatekeeper CAC

This topic describes how to implementing CAC on a gatekeeper.



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                                                                                                                                                |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>interzone</b>      | Total amount of bandwidth for H.323 traffic from the zone to any other zone                                                                                |
| <b>total</b>          | Total amount of bandwidth for H.323 traffic allowed in the zone                                                                                            |
| <b>session</b>        | Maximum bandwidth allowed for a session in the zone                                                                                                        |
| <b>default</b>        | Default value for all zones                                                                                                                                |
| <b>zone</b>           | A particular zone                                                                                                                                          |
| <b>zone-name</b>      | Name of the particular zone                                                                                                                                |
| <b>bandwidth-size</b> | Maximum bandwidth, in kbps<br>For <b>interzone</b> and <b>total</b> , the range is from 1 to 10,000,000. For <b>session</b> , 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                                                |
|-----------------------|------------------------------------------------------------|
| <b>bandwidth-size</b> | 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](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tvr/vrg_b1.htm#wp1503256).

## Implementing Gatekeeper CAC (Cont.)

Cisco.com

```
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 SJC GW
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGW v1.0—5-10

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

Cisco.com

**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.

© 2005 Cisco Systems, Inc. All rights reserved. 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.



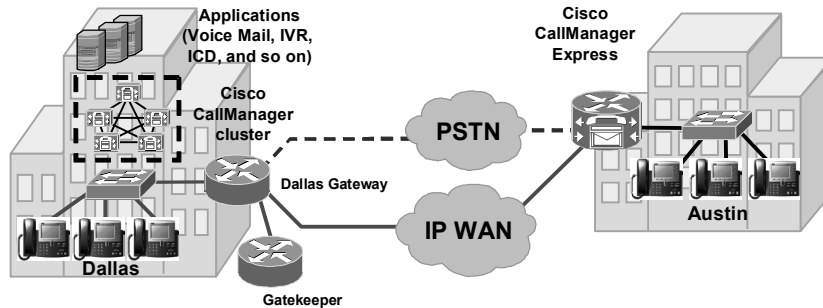
- You can provide gatekeeper redundancy by using gatekeeper clustering (alternate gatekeeper) or HSRP. Use HSRP only if gatekeeper clustering is not available in your software feature set.

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

© 2005 Cisco Systems, Inc. All rights reserved.

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 relatively 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.

© 2005 Cisco Systems, Inc. All rights reserved.

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](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a0080169445.shtml).

## Configuring Gatekeeper-Controlled Trunks in Cisco CallManager (Cont.)

Cisco.com

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration  
For Cisco IP Telephony Solutions

**Gatekeeper Configuration**

[Add a New Gatekeeper](#)  
[Back to Find/List Gatekeepers](#)  
[Dependency Records](#)

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                      | <input checked="" type="checkbox"/> |

\* indicates required item

© 2005 Cisco Systems, Inc. All rights reserved.

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: Protocal: H.223

Status: Ready

**Device Information**

|                           |                    |
|---------------------------|--------------------|
| Device Name*              | DFW_H225_Trunk     |
| Description               | h225_Trunk         |
| Device Pool*              | Device_Pool_AD_IHQ |
| 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 Termination 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

© 2005 Cisco Systems, Inc. All rights reserved.

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     |

© 2005 Cisco Systems, Inc. All rights reserved.

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 RASignalAddr 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)

© 2005 Cisco Systems, Inc. All rights reserved.

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

|                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Show commands:</b> <ul style="list-style-type: none"><li>• show gatekeeper gw-type-prefix</li><li>• show gatekeeper status</li><li>• show gatekeeper zone prefix</li><li>• show gatekeeper calls</li><li>• show gatekeeper endpoints</li><li>• show gatekeeper zone status</li></ul> | <b>Debug commands:</b> <ul style="list-style-type: none"><li>• debug h225 {asn1   events}</li><li>• debug h245 {asn1   events}</li><li>• debug proxy h323 statistics</li><li>• debug ras</li><li>• debug gate main [5] [10]</li></ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

© 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](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/323config/4gwconf.htm#wp1124639](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323config/4gwconf.htm#wp1124639)

Designing a Scaleable Dial Plan:

- [http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/dp3\\_isd.htm](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](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](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.

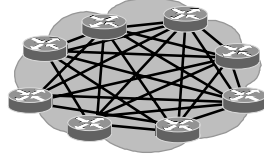
By using a directory gatekeeper, it is no longer necessary to have a full mesh between gatekeepers, which is a major advantage. Directory gatekeepers centralize the dial plan and also serve as a potential interface to other centralized applications. In a large-scale VoIP network, a centralized interface 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

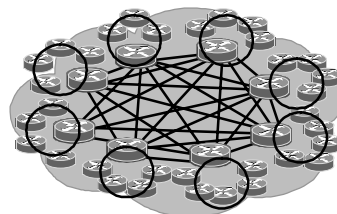
1. Small Network—Gateways Only



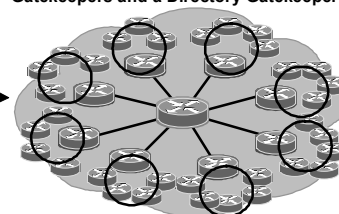
2. Small Network—Simplified with a Gatekeeper



3. Medium Network—Multiple Gatekeepers



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



© 2005 Cisco Systems, Inc. All rights reserved.

GWOK 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.

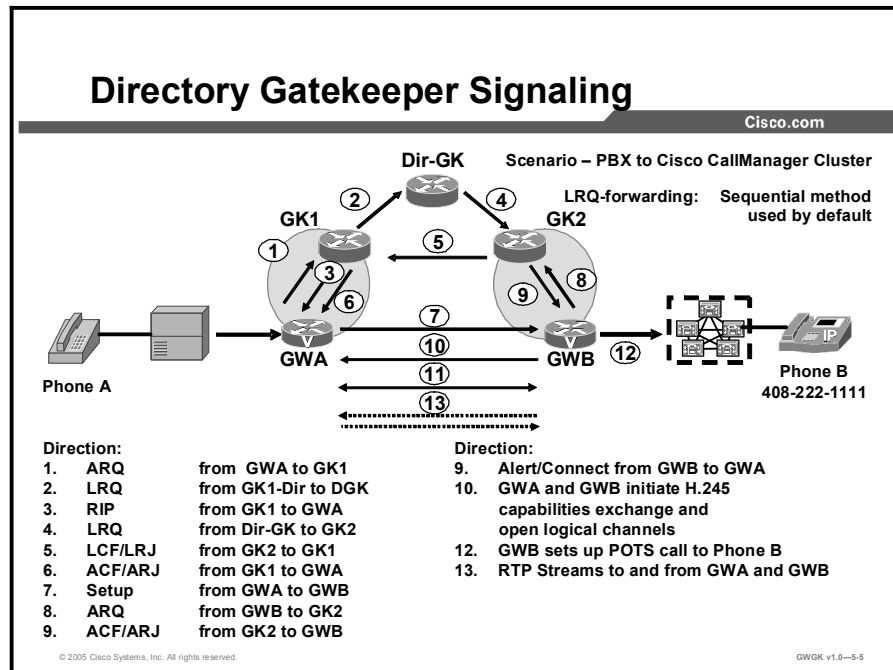
When adding a directory gatekeeper to a network, consider the following:

- 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.



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.



## 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 command 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.

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-57

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

© 2005 Cisco Systems, Inc. All rights reserved.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 RASignalAddr 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)

-
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 0
milan.xyz.co xyz.com 10.0.0.0 1719 RS 0 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:



```

 canMapAlias TRUE
 }
*Nov 29 08:13:22.242: H225 NONSTD INCOMING ENCODE BUFFER ::=
82899000110000000000
00000000000000000000000000F014005004400460057002D0047004B
*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
00000000000000000000000000000000F014005004400460057002D0047004B
*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 '8209900011000000000000000000000000000000000000... '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
cceded, 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.**

© 2005 Cisco Systems, Inc. All rights reserved.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](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](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](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](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

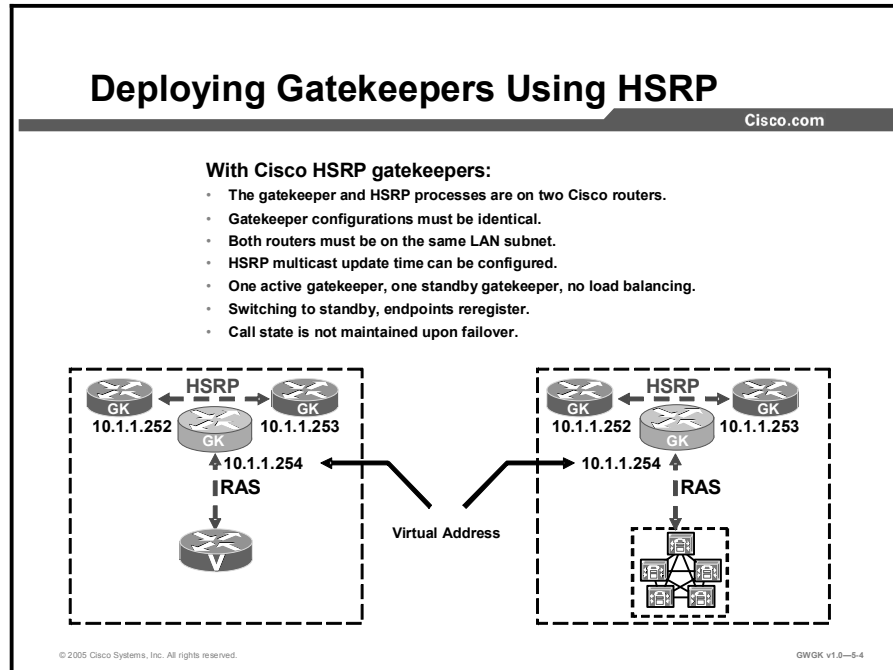
© 2005 Cisco Systems, Inc. All rights reserved.GWGK v1.0—5-3

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.



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                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <pre>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</pre> | The timers are very important. If these values are not set to the same number in both routers, HSRP will not function properly. |
| <pre>standby 1 priority 110</pre>                                                                                                           | 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                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>interface fastethernet 0/1  ip address 10.1.1.253 255.255.255.0  standby 1 ip 10.1.1.254  standby 1 preempt</pre> | 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. |
| <pre>standby 1 timers 5 15</pre>                                                                                       | 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
```

Configured on interface required

© 2005 Cisco Systems, Inc. All rights reserved. GWGK v1.0-5.8

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.

---



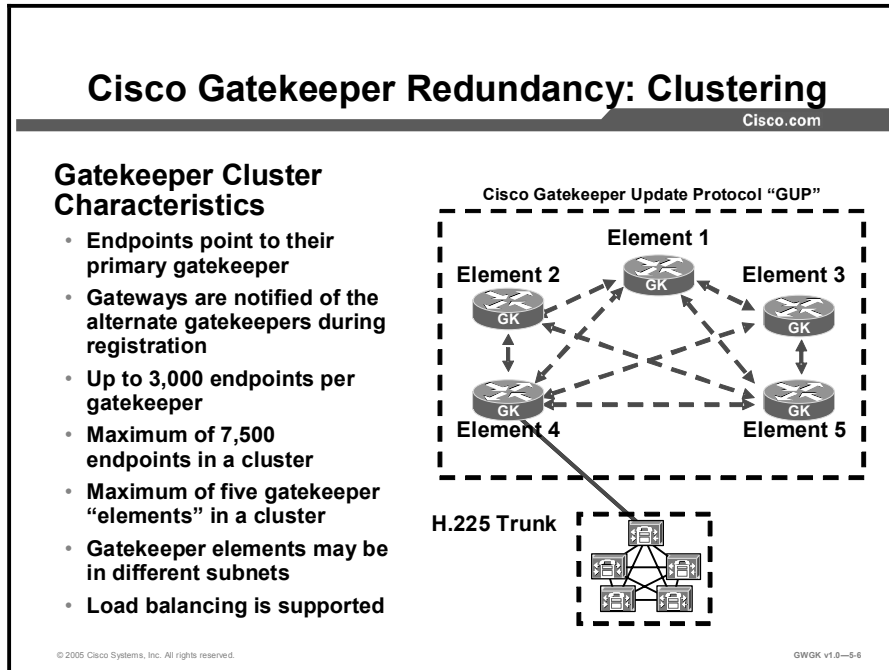
If the gatekeeper fails to send an registration confirmation (RCF) message back to the gateway, the gateway sends an RRQ message to the alternate gatekeeper. The alternate gatekeeper can be geographically independent in an IP network, but delay issues may arise if it is configured over long distances. 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.



## 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

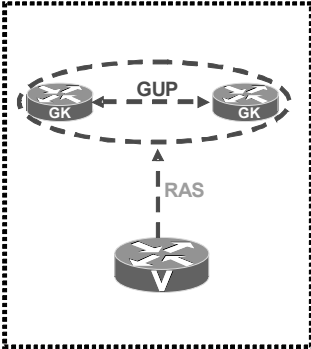
This topic describes how to implement gatekeeper clustering.

## 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



The diagram illustrates a gatekeeper cluster. At the top, two gatekeeper icons labeled 'GK' are connected by a double-headed arrow labeled 'GUP', indicating information sharing. Below them, a single gatekeeper icon labeled 'RAS' is connected to the cluster by a dashed arrow pointing upwards, representing the registration agent server.

© 2005 Cisco Systems, Inc. All rights reserved. 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.

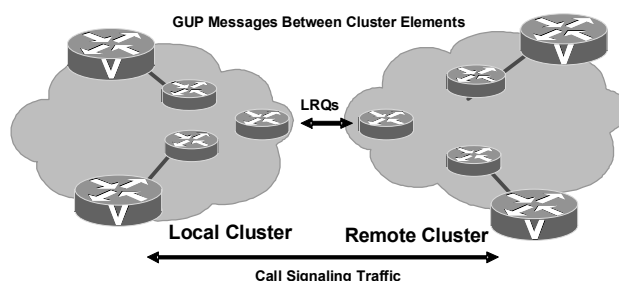
Within the zone, the cluster shares information about the following elements:

- 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.)

Cisco.com



**GUP announcements mean intelligent load sharing**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-5.8

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
```

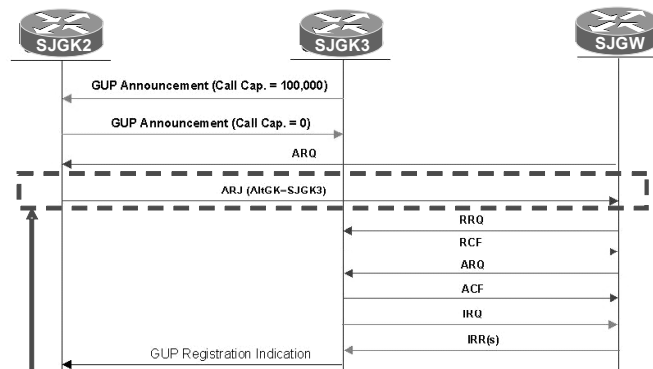
```
Router(config-gk)#zone prefix SJCluster 408*
```

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



**The SJK2 that is out of resource informs the SJGW to register to the Alternate SJK3.**

© 2005 Cisco Systems, Inc. All rights reserved.

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=SJK3). 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.



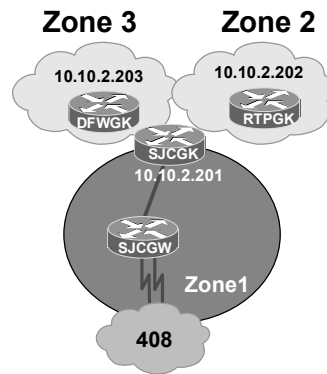
## US-GK Cluster Configuration

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
```



© 2005 Cisco Systems, Inc. All rights reserved.

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:

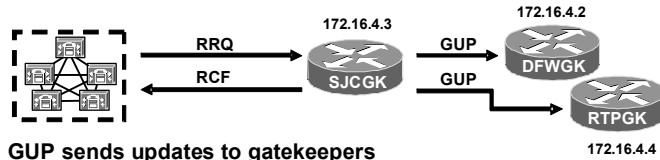
```
gatekeeper
zone local RTPGK1 cisco.com
zone cluster local RTPCluster RTPGK1
element RTPGK2 209.165.200.101 1719
element RTPGK3 209.165.200.102 1719
zone cluster remote SJCCluster cisco.com
element SJCGK1 209.18.79.23 1719
element SJCGK2 209.18.79.24 1719
element SJCGK3 209.18.79.25 1719
```

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

Cisco.com



**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

© 2005 Cisco Systems, Inc. All rights reserved.

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.**

© 2005 Cisco Systems, Inc. All rights reserved.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](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](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) v1.0 <http://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/323conf/5gkconf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323conf/5gkconf.htm)
- *Understanding Cisco IOS Software Gatekeeper Call Routing.*  
[http://www.cisco.com/en/US/tech/tk652/tk701/technologies\\_tech\\_note09186a00800a8928.shtml](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/ios123/123cger/vvfax\\_c/calle\\_c/h323\\_c/323conf/4gwconf.htm#wp1124639](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cger/vvfax_c/calle_c/h323_c/323conf/4gwconf.htm#wp1124639).
- *Designing a Scaleable Dial Plan.*  
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/dp3\\_isd.htm](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](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](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](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](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](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/ios123/123cger/vcl.htm>.
- *Cisco IOS Software Library 12.3 T H.323 Gateway Configuration.*  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cger/vvfax\\_c/calle\\_c/h323\\_c/323conf/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cger/vvfax_c/calle_c/h323_c/323conf/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.

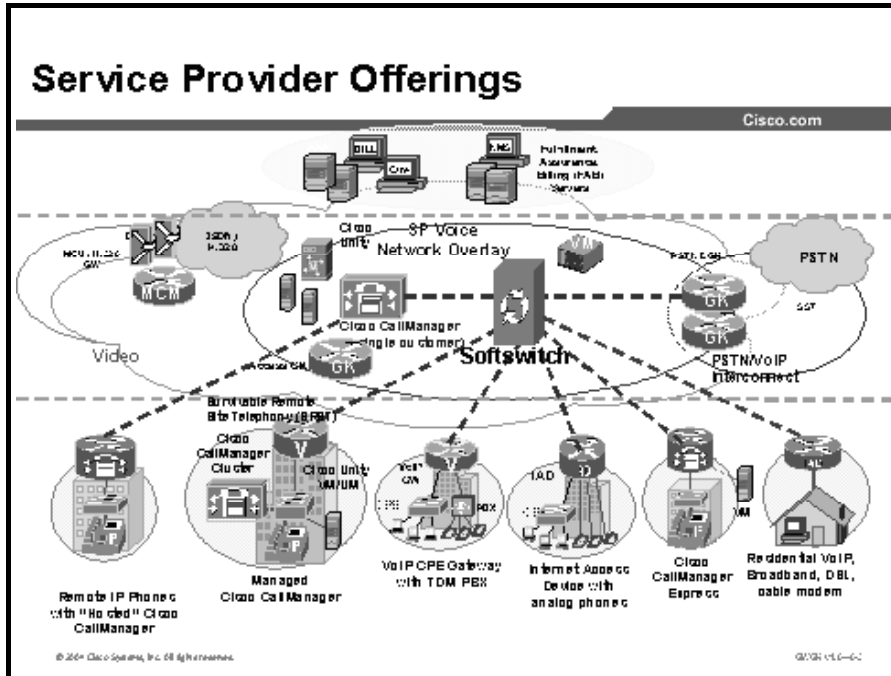
## Objectives

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

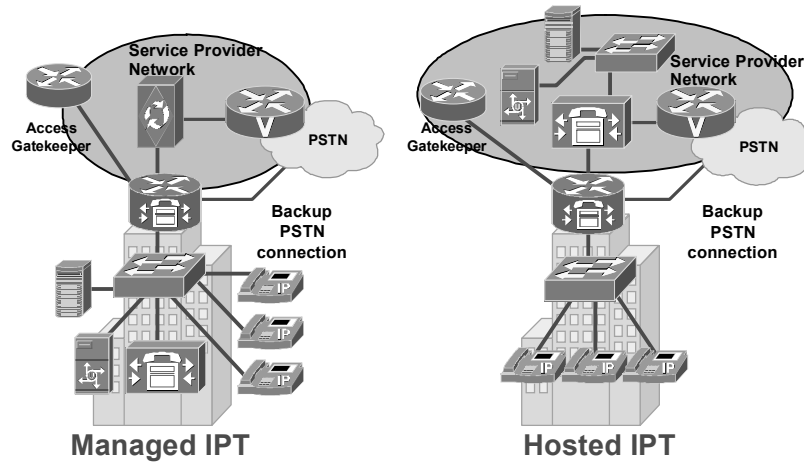
This topic describes common service provider offerings such as hosted and managed IP telephony services.



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.)

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

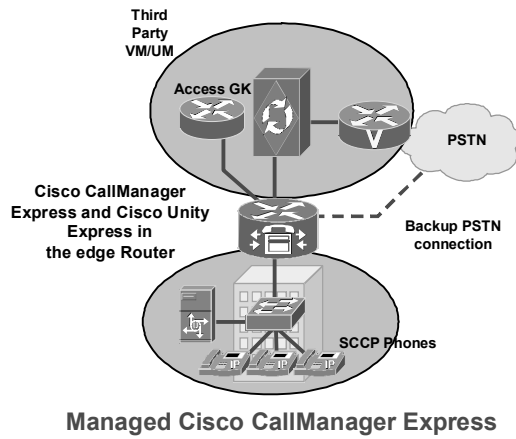
GWGK v1.0-6.4

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 either 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



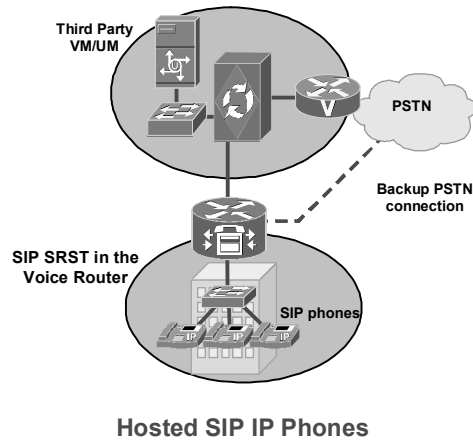
© 2005 Cisco Systems, Inc. All rights reserved.

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.)

Cisco.com



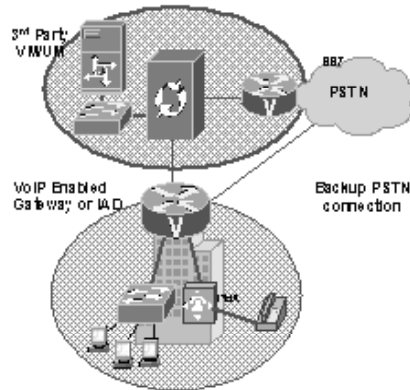
© 2005 Cisco Systems, Inc. All rights reserved.

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.)

Cisco.com



Managed Gateway with Internet Access Device (IAD)

© 2004 Cisco Systems, Inc. All rights reserved.

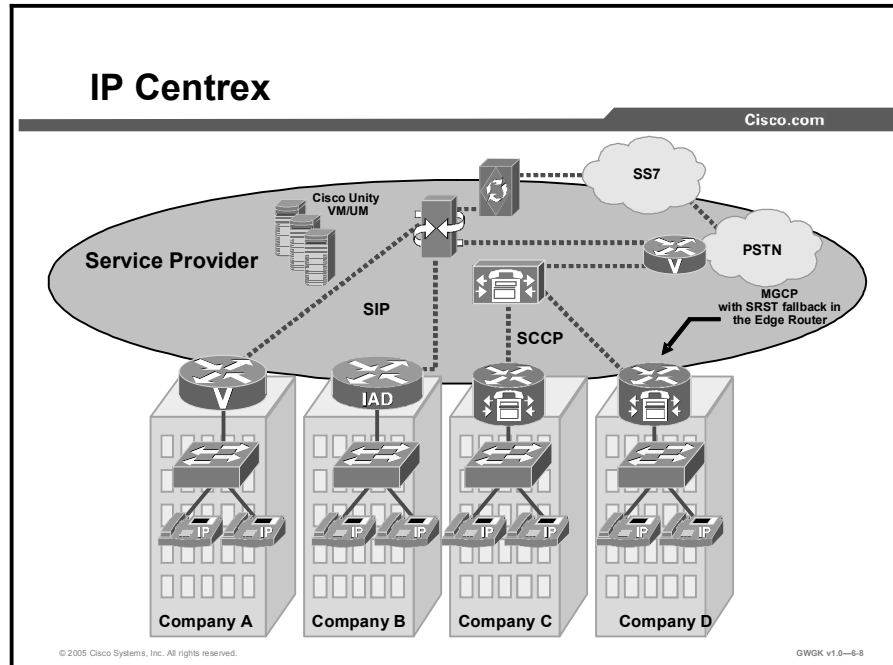
GWGK v1.0-07

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.

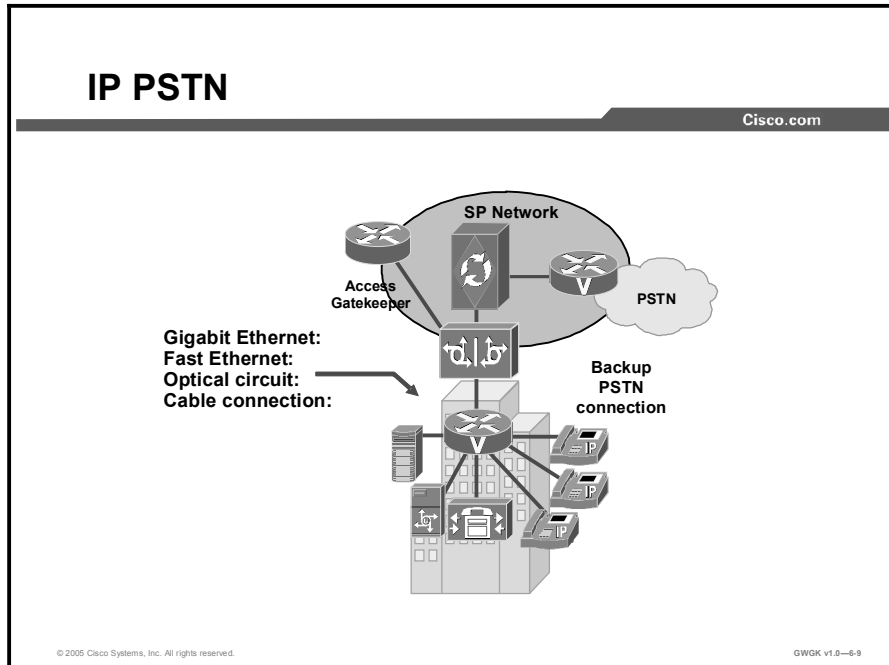


IP Telephony also can be provided as a hosted service from a shared server housed by the service provider, an approach sometimes referred to as IP Centrex. This figure shows a typical IP Centrex scenario where autonomous clients rent Centrex-like services like conferencing, call waiting, and call forwarding, 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

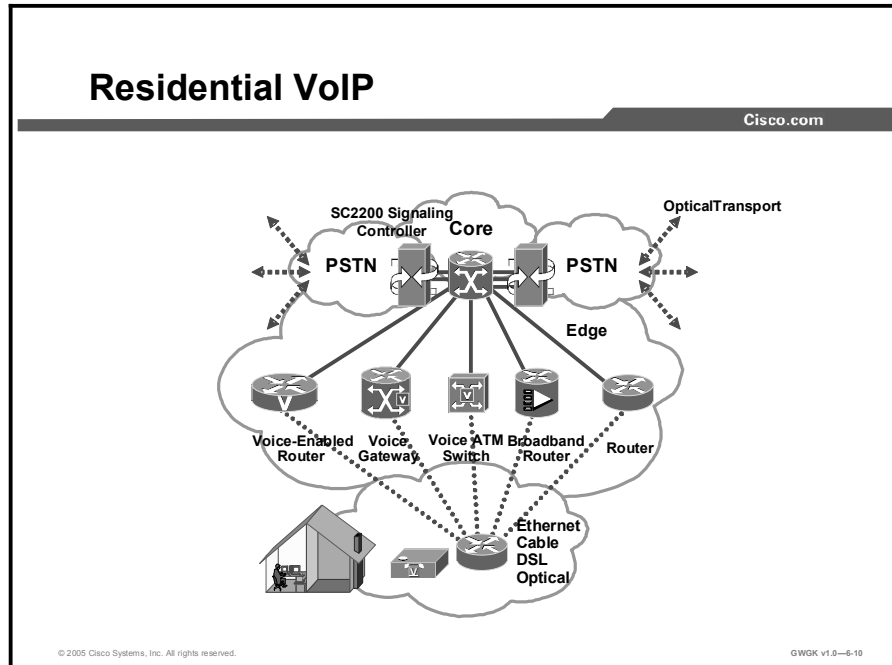
This topic describes IP PSTN services.



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

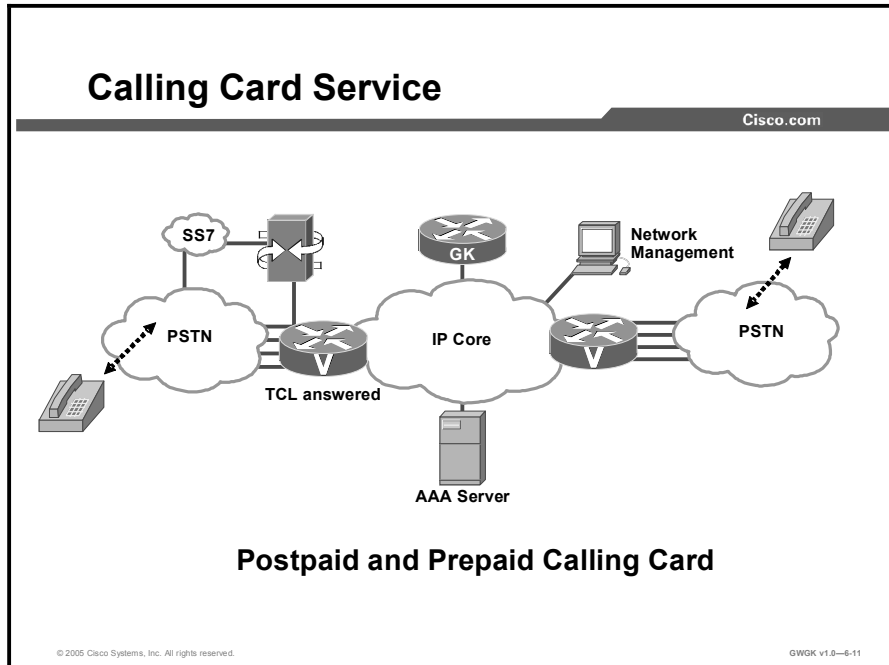
This topic describes residential VoIP.



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 providers 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.



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.

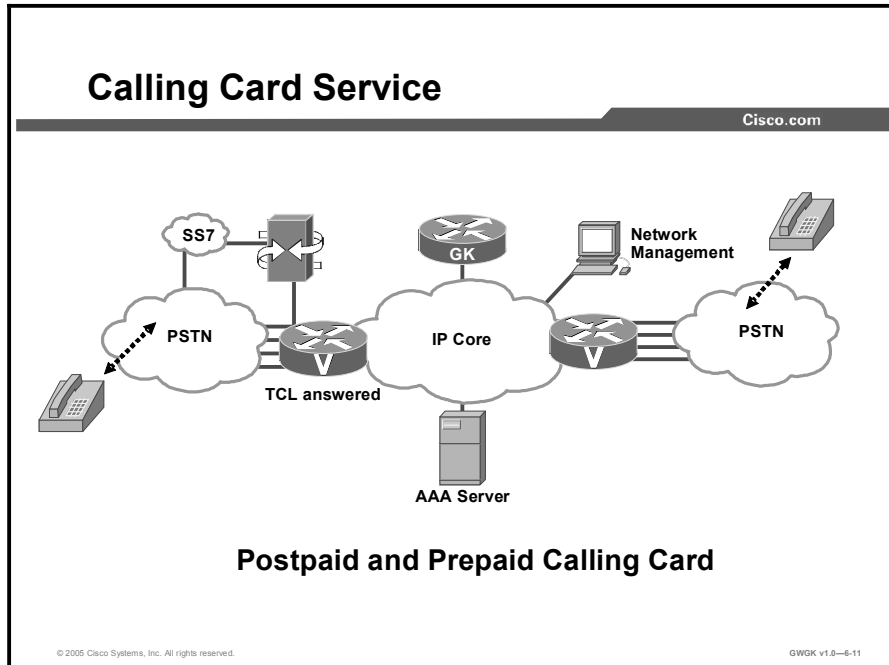
Postpaid calling-card services offer subscribers ongoing access to the long-distance network. As with prepaid calling cards, the postpaid service is often hosted by a wholesale carrier to improve profitability. The main difference between prepaid and postpaid calling-card services is that service authorizations 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.



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. GWOK v1.0-8-13

# 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

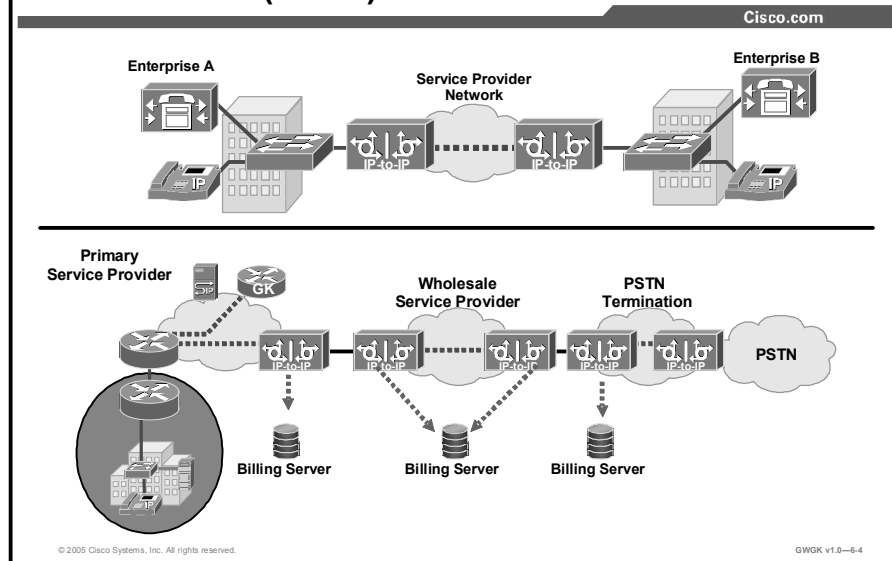
- **A demarcation point to establish efficient call CDR and billing**
- **A VoIP-to-VoIP gateway, currently supports H.323 to H.323 calls only**
- **A re-origination point for signaling and RTP media**
- **A way to replace back-to-back TDM gateways**
- **A gateway that typically exists in its own zone (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.)



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.)

Cisco.com

### 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**

© 2005 Cisco Systems, Inc. All rights reserved.

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.

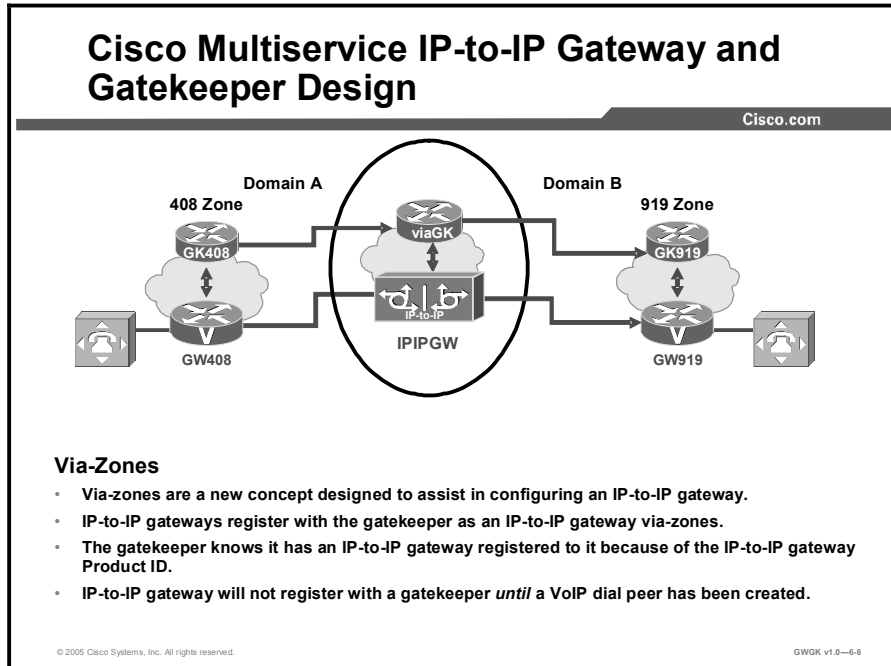
Existing Cisco 2600XM, 2800, 3660, 3745, 3725, and 3800 series router platforms can be used with the later versions of Cisco IOS software for the IP-to-IP gateway. However, the “classic” (non-XM) Cisco 2600 series platforms are not supported, and customers are required to upgrade to Cisco 2600XM Series 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.



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
```

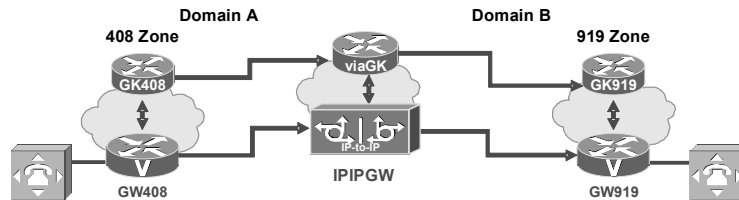
### GW919 Gateway

```
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

© 2005 Cisco Systems, Inc. All rights reserved.

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.**

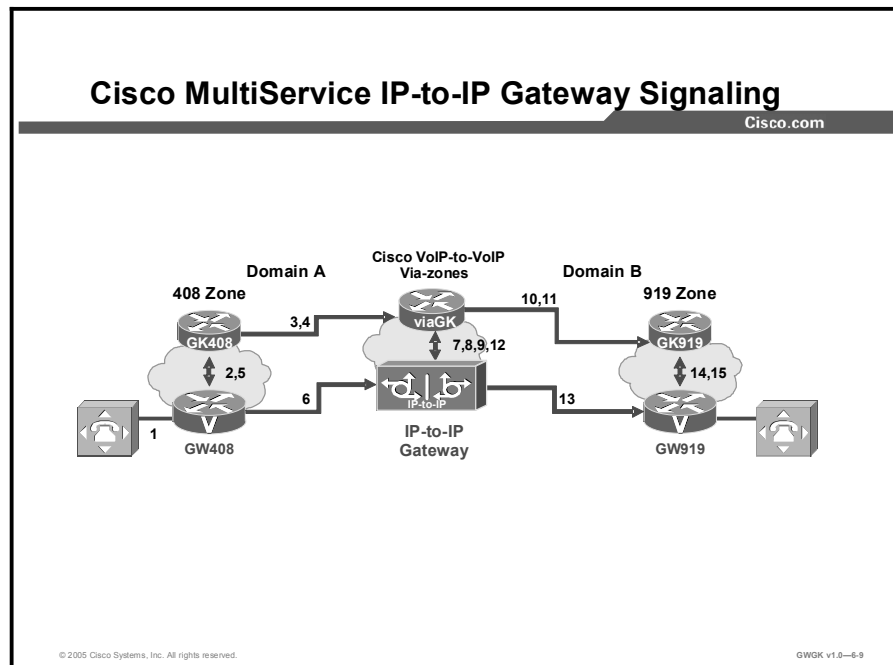
© 2005 Cisco Systems, Inc. All rights reserved.

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.



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. GK919 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.

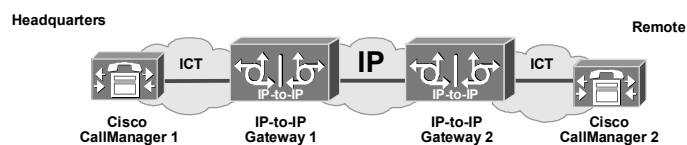
All other messages (for example, proceeding, alerting, and connect) are created as two call legs between GW408 and GW919, with the IP-to-IP gateway acting as an intermediate gateway.



## Cisco Multiservice IP-to-IP Gateway Signaling (Cont.)

Cisco.com

### IP-to-IP Gateway and Cisco CallManager Signaling



© 2005 Cisco Systems, Inc. All rights reserved.

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.

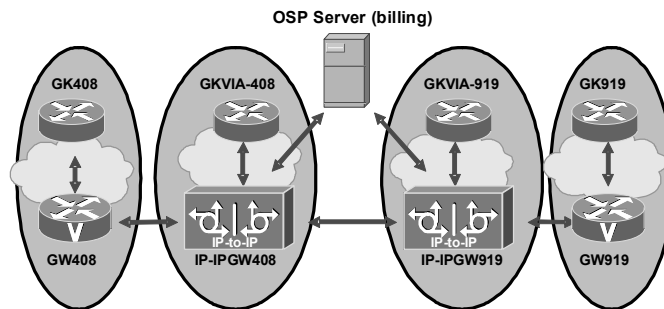
The following scenario, as illustrated in the figure, shows a basic call placed from a company headquarters to its remote office using Cisco CallManager and two Cisco Multiservice IP-to-IP Gateways.

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.



© 2005 Cisco Systems, Inc. All rights reserved.

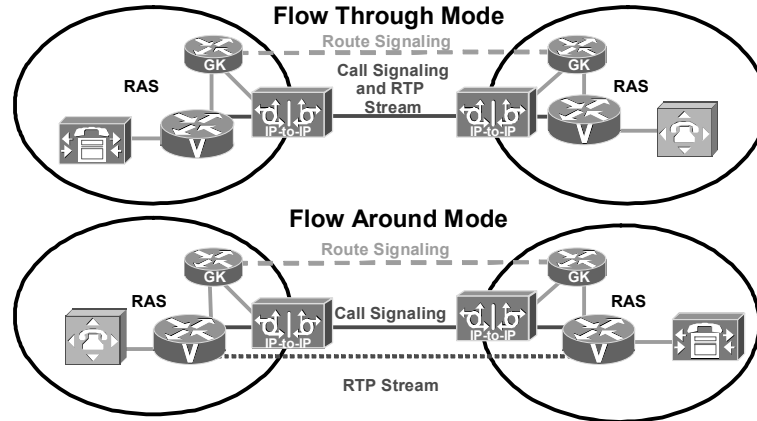
GWGK v1.0-6-11

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.)

Cisco.com



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-5-12

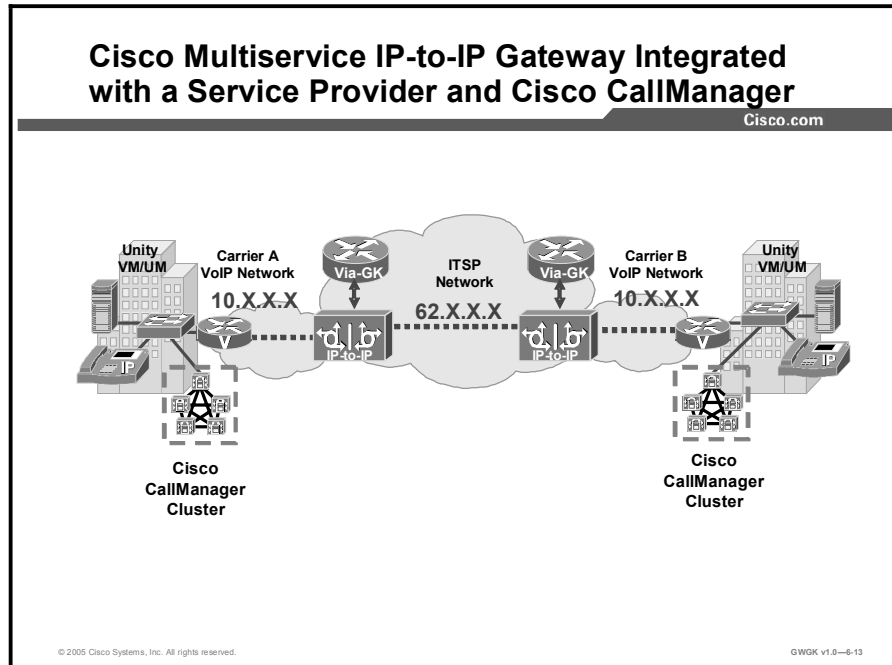
Flow through mode is a mode where the IP-to-IP gateway manages and supports not only the call setup but also the RTP streaming for a voice or video call. Flow around mode, on the other hand, is an alternate option that requires the IP-to-IP gateway to manage only the call setup, and the two endpoints 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.



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

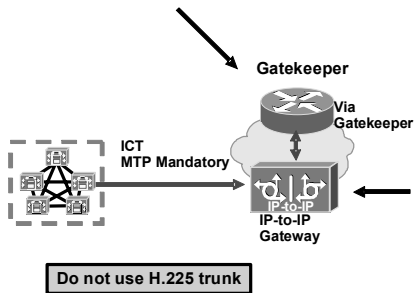
Cisco Multiservice IP-to-IP Gateway can be configured to do the following:

- 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.)

Cisco.com

```
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
```

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-5-14

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

The screenshot shows two configuration panels. The left panel, titled 'Trunk Configuration', shows 'Device Information' with fields for Device Name (IP-CPW), Description (IP-CPW), Device Pool (Device\_Pool\_AB\_HQ), Call Classification (OnNet), Media Resource Group List (DFW\_Main\_NRG), Location (HQ), AAR Group (DFW), and Turned Protocol (<None>). A checkbox 'Media Termination Point Required' is checked and labeled 'Mandatory'. Other checkboxes include 'Retry Video Call as Audio' and 'Party Replacement Support'. The right panel, titled 'Call Routing Information', shows 'Inbound Calls' with fields for Significant Digits (4), Calling Search Space (DFW\_HQ\_Full\_CSS), and AAR Calling search space (DFW\_HQ\_Full\_CSS). It also has checkboxes for 'Redirecting Number IE Delivery - Inbound' and 'Enable Inbound FastStart'. The 'Outbound Calls' section has fields for Calling Party Selection (Originator), Calling Line ID Presentation (Allowed), and several fields for 'Called party IE number type unknown' and 'Calling party IE number type unknown', all set to 'Cisco CallManager'. It also has checkboxes for 'Display IE Delivery', 'Redirecting Number IE Delivery - Outbound', and 'Enable Outbound FastStart', along with a 'Codec For Outbound FastStart' dropdown set to 'G711 ulaw 64K'.

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:

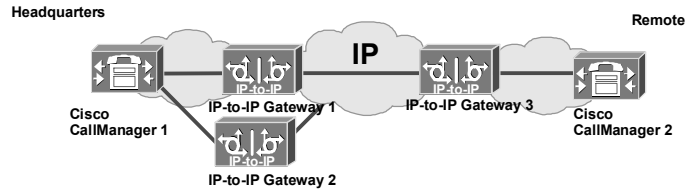
```
voice class h323 1
 call start fast
```

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*       | <input type="text" value="172.16.4.21"/> |
| Server 2 IP Address/Host Name        | <input type="text" value="172.16.4.22"/> |
| Server 3 IP Address/Host Name        | <input type="text"/>                     |

**IP-to-IP Gateway IP Address**

© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-5-16

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

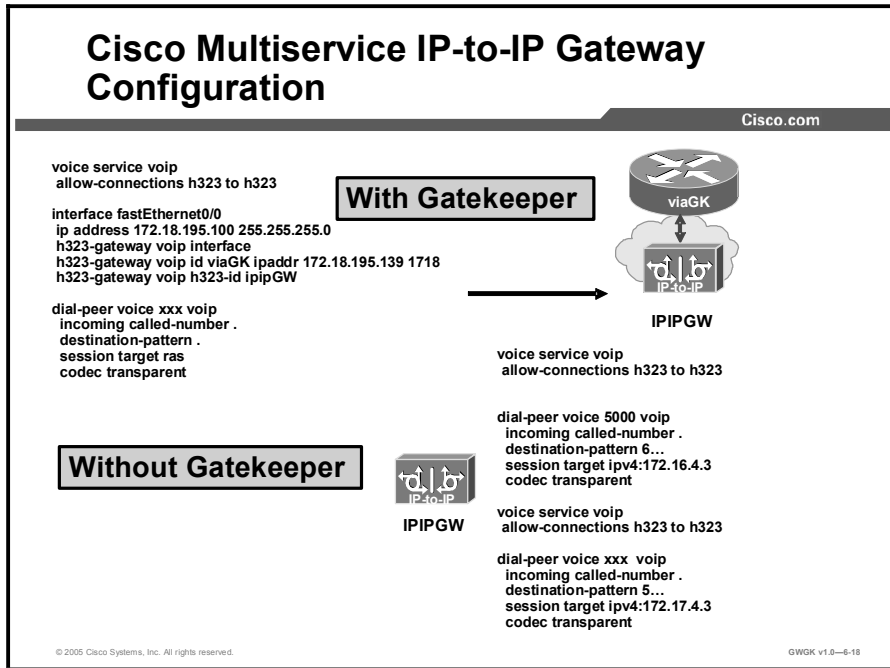
- **DTMF Relay:**
  - H.245 alphanumeric, H.245 signal, RFC 2833, and Cisco RTP DTMF relay types supported
  - Configuration is not needed on IP-to-IP Gateway
- **FAX Support**
  - T.38 fax relay
  - Fax pass-through
  - Cisco fax relay
  - Cisco proprietary NSE is not supported
- **TCL IVR version 2 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**

© 2005 Cisco Systems, Inc. All rights reserved. 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.



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.

© 2005 Cisco Systems, Inc. All rights reserved.GIWOK v1.0-8-19

## 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](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.**

© 2005 Cisco Systems, Inc. All rights reserved.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](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/ipipgw/index.htm).

**GWGK**

---

# Implementing Cisco Voice Gateways and Gatekeepers

---

Version 1.0

**Lab Guide**

CLS Production Services: 06.21.05

**Copyright © 2005, Cisco Systems, Inc. All rights reserved.**

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](http://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



Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

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.



# Lab Guide

---

## Overview

This guide presents the instructions and other information concerning the lab activities for this course. You can find the solutions in the lab activity Answer Key.

## Outline

This guide includes these activities:

- Lab 1-1: Configuring MGCP Gateways
- Lab 2-1: Configuring PSTN Connections
- Case Study 2-2: Migrating to IP Telephony from a PBX-Based System
- Lab 3-1: Implementing a Dial Plan and COR
- Lab 4-1: Configuring SRST
- Lab 4-2: Configuring DSP Farms
- Lab 4-3: Configuring TCL Scripts
- Lab 5-1: Configuring Gatekeepers
- Lab 5-2: Configuring Directory Gatekeepers
- Lab 6-1: Comprehensive Lab

# Lab 1-1: Configuring MGCP Gateways

Complete this lab activity to practice what you learned in the related module.

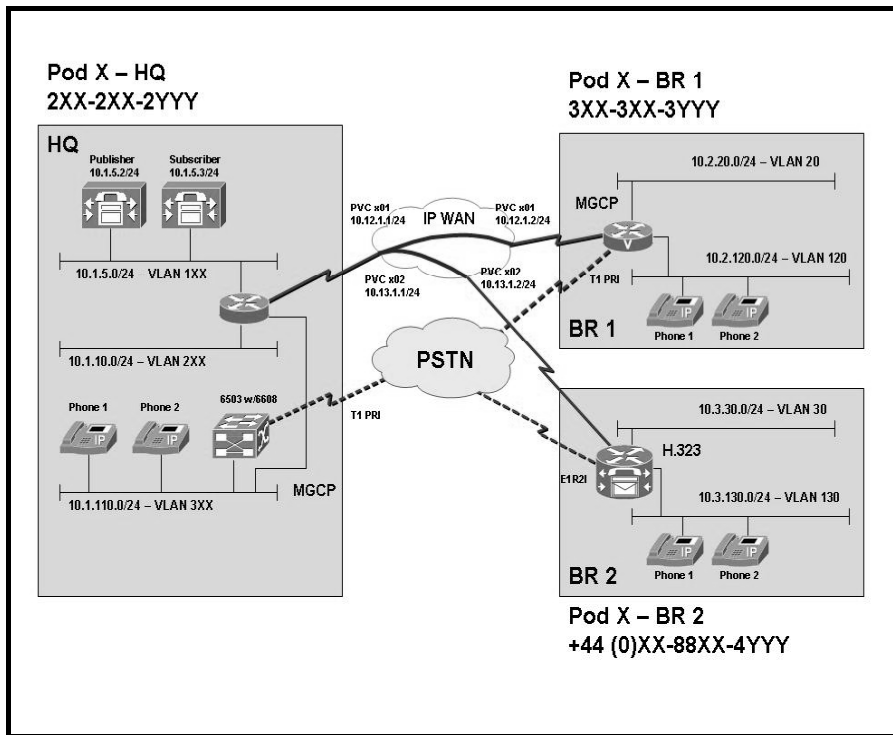
## Activity Objective

In this activity, you will be able to configure an MGCP gateway on a Cisco IOS software-based platform. After completing this activity, you will be able to meet these objectives:

- Configure and verify an MGCP gateway on a Cisco IOS software-based router and verify registration with a Cisco CallManager
- Configure MGCP gateways to support DTMF relay and fax pass-through

## Visual Objective

The figure illustrates what you will accomplish in this activity.



## Required Resources

These are the resources and equipment that are required to complete this activity:

### Student Pods

The student pod equipment requirements are as follows:

- Six Cisco IP Phones, which can be any model except for 7920. The IP Phones require power from either an in-line power switch or external power bricks.
- One Cisco router with one 10/100 Ethernet interface, one T1 serial interface, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one T1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one E1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco Catalyst 3550 switch for each branch location or one internal EtherSwitch module for the router.
- One Cisco Catalyst 6500 switch, one 10/100 Ethernet switch module, and one WS-X6608 gateway module for the HQ location.
- One Cisco CallManager publisher and one subscriber.

### Network Core

The network core equipment requirements are as follows:

- One Cisco router to provide Frame Relay or ATM support to an IP WAN to connect HQ with BR1 and BR2.
- One Cisco CallManager and one Cisco router configured as an MGCP gateway to provide the functionality of the PSTN to all locations.

## Command List

The table describes the commands that are used in this activity.

### MGCP and H.323 Commands

| Command                                     | Description                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ccm-manager fax protocol cisco</code> | <p>To enable the fax relay protocol for endpoints on a gateway, use the <b>ccm-manager fax protocol</b> command in global configuration mode. To disable the fax relay protocol, use the <b>no</b> form of this command.</p> <p>The command has this keyword:</p> <ul style="list-style-type: none"><li>■ <b>cisco</b>—Cisco-proprietary fax relay protocol. This is currently the only choice.</li></ul> |
| <code>ccm-manager mgcp</code>               | <p>To enable the gateway to communicate with Cisco CallManager through MGCP and to supply redundant control agent services, use the <b>ccm-manager mgcp</b> command in global configuration mode. To disable communication with Cisco CallManager and redundant control agent services, use the <b>no</b> form of this command.</p>                                                                       |

| Command                                                                                                                                                                                                                                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                               | This command has no arguments or keywords.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <pre> <b>ccm-manager redundant-host</b> { <i>ip-address</i>   <i>dns-name</i> } [ <i>ip-address</i>   <i>dns-name</i> ] </pre>                                                                                                                                                                | <p>To configure the IP address or the DNS name of one or two backup Cisco CallManager servers, use the <b>ccm-manager redundant-host</b> command in global configuration mode. To disable the use of backup Cisco CallManager servers as call agents, use the <b>no</b> form of this command.</p> <p>This command has these arguments:</p> <ul style="list-style-type: none"> <li>■ <i>ip-address</i>—IP address of the backup Cisco CallManager server</li> <li>■ <i>dns-name</i>—DNS name of the backup Cisco CallManager server</li> </ul>                                                                                                                              |
| <pre> <b>controller</b> { <i>t1</i>   <i>e1</i>   <i>ji</i> } <i>number</i> </pre>                                                                                                                                                                                                            | <p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> <li>■ <b>t1</b>—T1 controller.</li> <li>■ <b>e1</b>—E1 controller.</li> <li>■ <b>j1</b>—J1 controller.</li> </ul> <p><i>slot/port</i>—Backplane slot number and port number on the interface. Refer to your hardware installation manual for the specific values and slot numbers.</p> <p><i>number</i>—NPM number, in the range 0 through 2.</p>                                                                                                                                                                                                                                 |
| <pre> <b>dtmf-relay</b> [<b>cisco-rtp</b>] [<b>h245-alphanumeric</b>] [<b>h245-</b> <b>signal</b>] [<b>rtp-nte</b>] </pre>                                                                                                                                                                    | <p>Forwards DTMF tones.</p> <p>This command has these keywords:</p> <ul style="list-style-type: none"> <li>■ <b>cisco-rtp</b>—(Optional) Forwards DTMF tones by using RTP with a Cisco proprietary payload type.</li> <li>■ <b>h245-alphanumeric</b>—(Optional) Forwards DTMF tones by using the H.245 “alphanumeric” Ull method. Range: tones 0 to 9, *, #, and A to D. Use this keyword to configure DTMF relay.</li> <li>■ <b>h245-signal</b>—(Optional) Forwards DTMF tones by using the H.245 “signal” Ull method. Range: tones 0 to 9, *, #, and A to D.</li> <li>■ <b>rtp-nte</b>—(Optional) Forwards DTMF tones by using RTP with the NTE payload type.</li> </ul> |
| <pre> <b>exit</b> </pre>                                                                                                                                                                                                                                                                      | Exits the current mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <pre> <b>fax protocol pass-through</b> { <b>g711ulaw</b>   <b>g711alaw</b> }   <b>system</b> </pre> <p>or</p> <pre> <b>modem passthrough</b> { <b>system</b>   <b>nse</b> [<b>payload-type</b> <i>number</i>] <b>codec</b> { <b>g711alaw</b>   <b>g711ulaw</b> } [<b>redundancy</b>] } </pre> | <p>Specifies the type of fax protocol to use on this dial peer.</p> <p>This command has these keywords:</p> <ul style="list-style-type: none"> <li>■ <b>pass-through</b>—Uses the H.323 or SIP protocol stack and the G.711 u-law or G.711 a-law codec. Use the same codec type for the originating and terminating gateways.</li> <li>■ <b>system</b>—Uses the protocol set under the voice-service configuration mode.</li> <li>■ <b>g711alaw</b>—G.711 a-law codec type for E1.</li> </ul>                                                                                                                                                                              |

| Command                                                                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                         | <ul style="list-style-type: none"> <li>■ <b>g711ulaw</b>—G.711 u-law codec type for T1.</li> </ul> <p>Note: This command has other keywords and arguments that are used for T.38 fax relay. These keywords and arguments are described in the lesson “Configuring Fax and Modem Support.”</p> <p>or</p> <p>Enables faxes to use modem pass-through and NSEs for fax changeover signaling.</p> <p>This command has these keywords:</p> <ul style="list-style-type: none"> <li>■ <b>system</b>—Uses the protocol set under the voice-service configuration mode..</li> <li>■ <b>nse</b>—NSE signaling is used to communicate codec switchover.</li> <li>■ <b>payload-type number</b>—(Optional) Value for NSE payload type. Range varies by platform but is from 96 to 119 on most platforms. Default: 100.</li> <li>■ <b>codec</b>—Codec selection for upspeaking. Default: g711ulaw. Use the same codec type for the originating and terminating gateways. The two codec types are as follows: <ul style="list-style-type: none"> <li>— <b>g711alaw</b>—G.711 a-law codec type for E1</li> <li>— <b>g711ulaw</b>—G.711 u-law codec type for T1</li> </ul> </li> <li>■ <b>redundancy</b>—(Optional) Enables a single repetition of packets (using RFC 2198) to protect against packet loss.</li> </ul> |
| <b>fax-rate disable</b>                                                                                                 | (Optional) Disables fax protocol capability on this dial peer. Use this command only when you want to force faxes to use modem pass-through. Do not use this command when you want faxes to use fax pass-through or fax relay on this dial peer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <p>For T1 lines:</p> <pre>framing {sf   esf}</pre> <p>For E1 lines:</p> <pre>framing {crc4   no-crc4} [australia]</pre> | <p>Use this command in configurations in which the router or access server is intended to communicate with T1 or E1 fractional data lines. The service provider determines the framing type that is required for your T1 or E1 circuit.</p> <p>This command does not have a <b>no</b> form.</p> <p>This command has these keywords:</p> <ul style="list-style-type: none"> <li>■ <b>sf</b>—Specifies super frame as the T1 frame type. This is the default.</li> <li>■ <b>esf</b>—Specifies extended super frame as the T1 frame type.</li> <li>■ <b>crc4</b>—Specifies CRC4 frame as the E1 frame type. This is the default for Australia.</li> <li>■ <b>no-crc4</b>—Specifies no CRC4 frame as the E1 frame type.</li> <li>■ <b>australia</b>— (Optional) Specifies the E1 frame type that is used in Australia.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Command                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>interface type number [nametag]</code> | <p>Enters interface configuration mode for the interface that is connected to the gatekeeper.</p> <p>This command has these arguments:</p> <ul style="list-style-type: none"> <li>■ <i>type</i>—Type of interface to be configured.</li> <li>■ <i>number</i>—Port, connector, or interface card number. The number is assigned at the factory at the time of installation or when added to a system, and can be displayed with the <b>show interfaces</b> command.</li> <li>■ <i>nametag</i>—(Optional) Logic name to identify the server configuration so that multiple entries of server configuration can be entered.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>ip cef</code>                          | (Optional) Enables Cisco Express Forwarding routing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <code>linecode {ami   b8zs   hdb3}</code>    | <p>Use this command in configurations in which the router or access server must communicate with T1 fractional data lines. The T1 service provider determines which line-code type, either <b>ami</b> or <b>b8zs</b>, is required for your T1 circuit. Likewise, the E1 service provider determines which line-code type, either <b>ami</b> or <b>hdb3</b>, is required for your E1 circuit.</p> <p>This command does not have a <b>no</b> form.</p> <p>This command has these keywords:</p> <ul style="list-style-type: none"> <li>■ <b>ami</b>—Specifies AMI as the line-code type. Valid for T1 or E1 controllers. This is the default for T1 lines.</li> <li>■ <b>b8zs</b>—Specifies B8ZS as the line-code type. Valid for T1 controller only.</li> <li>■ <b>hdb3</b>—Specifies HDB3 as the line-code type. Valid for E1 controller only. This is the default for E1 lines.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>mgcp [port]</code>                     | <p>The command has this argument:</p> <ul style="list-style-type: none"> <li>■ <i>port</i>—(Optional) The UDP ports for global call agent configuration (with this command) and call agent configuration for an MGCP profile (with the <b>mgcp profile call-agent</b> command) are mutually exclusive; the first is configured on an endpoint blocks configuration of the other on the same endpoint.</li> </ul> <p>Identifying call agents by DNS name rather than by IP address in the <b>mgcp call-agent</b> and <b>mgcp profile call-agent</b> commands provides call agent redundancy, because a DNS name can have more than one IP address associated with it. If a call agent is identified by DNS name and a message from the gateway fails to reach the call agent, the <b>max1 lookup</b> and <b>max2 lookup</b> commands enable a search from the DNS lookup table for a backup call agent at a different IP address.</p> <p>The <i>port</i> argument configures the call agent port number (the UDP port over which the gateway sends messages to the call agent). The reverse (the gateway port number, or the UDP port over which the gateway receives messages from the call agent) is configured by specifying a port number in the <b>mgcp</b> command.</p> <p>When the service type is set to <i>mgcp</i>, the call agent processes the RSIP error messages sent by the gateway if</p> |

| Command                                                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                          | <p>the <b>mgcp sgcp restart notify</b> command is enabled. When the service type is set to <i>sgcp</i>, the call agent ignores the RSIP messages.</p> <p>Use this command on any platform and media gateway.</p> <p>The <i>mgcp</i> service type supports the RSIP error messages that are sent by the gateway if the <b>mgcp sgcp restart notify</b> command is enabled.</p> <p>The range for the MGCP gateway is from 1025 to 65535. The default is UDP port 2427.</p> <p>Once you start the MGCP daemon using the <b>mgcp</b> command, you can suspend it (for example, for maintenance) by using the <b>mgcp block-newcalls</b> command. When you are ready to resume normal MGCP operations, use the <b>no mgcp block-newcalls</b> command. Use the <b>no mgcp</b> command only if you intend to terminate all MGCP applications and protocols.</p> <p>When the MGCP daemon is not active, all MGCP messages are ignored.</p> <p>If you want to change the UDP port while MGCP is running, you must stop the MGCP daemon using the <b>no mgcp</b> command, and then restart it with the new port number using the <b>mgcp port</b> command.</p>                                                                                                                                                                                                                                                                                                                         |
| <pre>mgcp call-agent {dns-name   ip-address} [port] [service-type type] [version protocol-version]</pre> | <p>To configure the address and protocol of the call agent for MGCP endpoints on a media gateway, use the <b>mgcp call-agent</b> command in global configuration mode. To reset to the default, use the <b>no</b> form of this command.</p> <p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> <li>■ <i>dns-name</i>—Fully qualified domain name (including host portion) for the call agent; for example, ca123.example.net.</li> <li>■ <i>ip-address</i>—IP address for the call agent.</li> <li>■ <b>service-type type</b>—(Optional) Type of gateway control service protocol. It can be one of these values: <ul style="list-style-type: none"> <li>— <i>mgcp</i>—Media Gateway Control Protocol</li> <li>— <i>ncs</i>—Network Communication Server</li> <li>— <i>sgcp</i>—Simple Gateway Control Protocol</li> <li>— <i>tgcp</i>—Trunking Gateway Control Protocol</li> </ul> </li> <li>■ <b>version protocol-version</b>—(Optional) Version of gateway control service protocol. It can be one of these values: <ul style="list-style-type: none"> <li>— For service-type <i>mgcp</i>: <ul style="list-style-type: none"> <li>0.1—Version 0.1 of MGCP (Internet Draft)</li> <li>1.0—Version 1.0 of MGCP (RFC 2705 version 1.0)</li> </ul> </li> </ul> </li> </ul> <p>Note: This configuration value is used to allow the router to tailor the MGCP application behavior to be compatible based on the RFC 2705 definitions.</p> |

| Command | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <ul style="list-style-type: none"> <li>— For <b>service-type ncs</b>: 1.0</li> <li>— For <b>service-type sgcp</b>: 1.1, 1.5</li> <li>— For <b>service-type tgcp</b>: 1.0</li> </ul> <p>Global call agent configuration (with this command) and call agent configuration for an MGCP profile (with the <b>mgcp profile call-agent</b> command) are mutually exclusive; the first is configured on an endpoint blocks configuration of the other on the same endpoint.</p> <p>Identifying call agents by DNS name rather than by IP address in the <b>mgcp call-agent</b> and <b>mgcp profile call-agent</b> commands provides call agent redundancy, because a DNS name can have more than one IP address associated with it. If a call agent is identified by DNS name and a message from the gateway fails to reach the call agent, the <b>max1 lookup</b> and <b>max2 lookup</b> commands enable a search from the DNS lookup table for a backup call agent at a different IP address.</p> <p>The <i>port</i> argument configures the call agent port number (the UDP port over which the gateway sends messages to the call agent). The reverse (the gateway port number, or the UDP port over which the gateway receives messages from the call agent) is configured by specifying a port number in the <b>mgcp</b> command.</p> <p>When the service type is set to <i>mgcp</i>, the call agent processes the RSIP error messages sent by the gateway if the <b>mgcp sgcp restart notify</b> command is enabled. When the service type is set to <i>sgcp</i>, the call agent ignores the RSIP messages.</p> <p>Use this command on any platform and media gateway.</p> <p>The <i>mgcp</i> service type supports the RSIP error messages sent by the gateway if the <b>mgcp sgcp restart notify</b> command is enabled.</p> |



| Command                                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>mgcp dtmf-relay voip codec {all   low-bit-rate} mode {cisco   nse   out-of-band    nte-gw   nte-ca}</pre> | <p>This command has these keywords:</p> <ul style="list-style-type: none"> <li>■ <b>voip</b>—VoIP calls.</li> <li>■ <b>voaal2</b>—VoAAL2 calls (using Annex K type 3 packets).</li> <li>■ <b>all</b>—DTMF relay is to be used with all voice codecs.</li> <li>■ <b>low-bit-rate</b>—DTMF relay is to be used with only low-bit-rate voice codecs, such as G.729.</li> <li>■ <b>cisco</b>—RTP digit events are encoded using a proprietary format similar to Frame Relay as described in the FRF.11 specification. The events are transmitted in the same RTP stream as nondigit voice samples, using payload type 121.</li> <li>■ <b>nse</b>—NSE RTP digit events are encoded using the format that is specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples, using the payload type that is configured using the <b>mgcp tse payload</b> command.</li> <li>■ <b>out-of-band</b>—MGCP digit events are sent using NTFY messages to the call agent, which plays them on the remote gateway using RQNT messages with “S:” (signal playout request).</li> <li>■ <b>nte-gw</b>—RTP digit events are encoded using the NTE format that is specified in RFC 2833, Section 3.0, and are transmitted in the same RTP stream as nondigit voice samples. The payload type is negotiated by the gateways before use. The configured value for payload type is presented as the preferred choice at the beginning of the negotiation.</li> <li>■ <b>nte-ca</b>—Identical to the <b>nte-gw</b> keyword behavior except that the local connection options “a:” line of the call agent is used to enable or disable DTMF relay.</li> </ul> <p>Use this command to access an announcement server or a voice-mail server that cannot decode RTP packets that contain DTMF digits. When the <b>mgcp dtmf-relay</b> command is active, the DTMF digits are removed from the voice stream and carried so that the server can decode the digits.</p> <p>Only VoIP supports the <b>mode</b> keyword for forwarding digits on codecs.</p> |

| Command                                                                                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>show ccm-manager [backhaul   config-download   fallback-mgcp   hosts   music-on-hold   redundancy   download-tones [c1   c2]]</pre> | <p>To display a list of Cisco CallManager servers and their current status and availability, use the <b>show ccm-manager</b> command in privileged EXEC mode.</p> <p>This command has these keywords:</p> <ul style="list-style-type: none"> <li>■ <b>backhaul</b>—(Optional) Information about the backhaul link.</li> <li>■ <b>config-download</b>—(Optional) Displays information about the status of Media Gateway Control Protocol (MGCP) configuration download.</li> <li>■ <b>fallback-mgcp</b>—(Optional) Displays the status of the MGCP gateway fallback feature.</li> <li>■ <b>hosts</b>—(Optional) Displays a list of each configured Cisco CallManager server in the network, together with its operational status and host IP address.</li> <li>■ <b>music-on-hold</b>—(Optional) Displays information about all the multicast music-on-hold (MOH) sessions in the gateway at any given point in time.</li> <li>■ <b>redundancy</b>—(Optional) Displays failover mode and status information for hosts, including the redundant link port, failover interval, keepalive interval, MGCP traffic time, switchover time, and switchback mode.</li> <li>■ <b>download-tones [c1   c2]</b>—(Optional) Displays custom tones downloaded to the gateway. The custom tone value of c1 or c2 specifies which tone information to display.</li> </ul> |

## Job Aids

These job aids are available to help you complete the lab activity.

You will need a copy of Microsoft Remote Desktop Client for many of the labs in this course. If you do not have a copy of this application, contact your instructor for assistance in obtaining it.

### Lab 1-1 Job Aids

| Device          | IP Address |
|-----------------|------------|
| Terminal server | 10.1.10.50 |
| Publisher       | 10.1.5.2   |
| Subscriber      | 10.1.5.3   |

## Task 1: Configure MGCP Gateway

The Armstrong Snow Shovel Company has three offices. They are designated as Headquarters (HQ), Branch 1 (BR1), and Branch 2 (BR2). The firm initially started manufacturing snow shovels and now has a complete line of garden tools for the do-it-yourself market. HQ has a Cisco CallManager cluster with Cisco Unity voice mail. It also has a Cisco Catalyst 6500 switch with a WS-X6608-T1/E1 gateway blade. The DNs that are assigned at HQ are in the range defined in the topology figure. HQ has a T1 PRI to the PSTN and a 768K Frame Relay link to the IP WAN.

BR1 uses the Cisco CallManager cluster at HQ for call signaling and control. The gateways on this connection use MGCP to maximize call survivability. The gateway connection to the PSTN uses a T1 PRI setup for QSIG and a 768K Frame Relay connection to the IP WAN. The specific extension numbers for this site are in the topology figure.

BR2 is a new site with only a few users, but this site is expected to grow rapidly. Initially, this site will have a Cisco CallManager Express device to support the users. This location has an E1R2 CAS connection to the PSTN and a 768K Frame Relay connection to the IP WAN.

The data and voice network infrastructure has been deployed, as well as the Cisco CallManager cluster and Cisco Unity voice-mail server. You have been brought in to implement the MGCP gateway for this customer.

### Activity Procedure

Complete these steps:

- Step 1** Connect your PC to the switch port on one of the HQ Cisco IP Phones and use Telnet to access the communications server using the IP address supplied in the previous table.
- Step 2** Configure MGCP on the gateway at BR1. The gateway has been defined in the Cisco CallManager cluster at HQ for you.
- Step 3** Ensure accurate forwarding of digits on compressed codecs. Pass dialed digits in the same RTP stream as nondigit voice samples.
- Step 4** Configure the gateway so that fax traffic is handled as a standard G.711 call.

### Activity Verification

You have completed this task when you attain these results:

- You are able to verify that the gateway at BR1 has registered as an MGCP gateway with the Cisco CallManager cluster at HQ.
- You are able to verify that the correct MGCP command has been entered in the gateway configuration to support DTMF relay and fax pass-through.

## Lab 1:1 Answer Key: Configuring MGCP Gateways

When you complete this activity, your configuration will be similar to the results here, with differences that are specific to your device or workgroup:

### Task 1 Solution

- Step 1** Connect your PC to a phone at HQ.
- Step 2** Enabling an MGCP gateway to register with Cisco CallManager requires configuration of the primary Cisco CallManager and enabling of MGCP. It is also recommended that a redundant Cisco CallManager be configured. Type these commands in BR1:
- ```
mgcp call-agent 10.1.5.3
ccm-manager mgcp
ccm-manager redundant-host 10.1.5.2
mgcp
```
- Step 3** Enable DTMF relay to ensure accurate forwarding of digits. Type this command in BR1:
- ```
mgcp dtmf-relay voip codec all mode cisco
```
- Step 4** By default, Cisco fax relay is enabled on an MGCP gateway. To handle fax calls as normal G.711 calls, fax relay must be disabled, which results in fax pass-through being used. Type this command in BR1:
- ```
no ccm-manager fax protocol cisco
```
- Step 5** Enter **show ccm-manager** to verify the MGCP status. Your output should be similar to these results:

```
Pod8-BR1#sh ccm-manager
MGCP Domain Name: Pod8-BR1
Priority          Status                      Host
=====
Primary          Registering with CM        10.1.5.3
First Backup     Backup Ready               10.1.5.2
Second Backup    None
Current active Call Manager:  None
Backhaul/Redundant link port: 2428
Failover Interval: 30 seconds
Keepalive Interval: 15 seconds
Last keepalive sent: 03:59:21 UTC Mar 20 2002
Last MGCP traffic time: 04:33:56 UTC Mar 22 2002
Last failover time: 04:33:26 UTC Mar 22 2002
from (10.1.5.3)
Last switchback time: 04:33:56 UTC Mar 22 2002
from (10.1.5.2)
Switchback mode: Graceful
MGCP Fallback mode: Not Selected
Last MGCP Fallback start time: None
Last MGCP Fallback end time: None
MGCP Download Tones: Disabled
```

Lab 2-1: Configuring PSTN Connections

Complete this lab activity to practice what you learned in the related module.

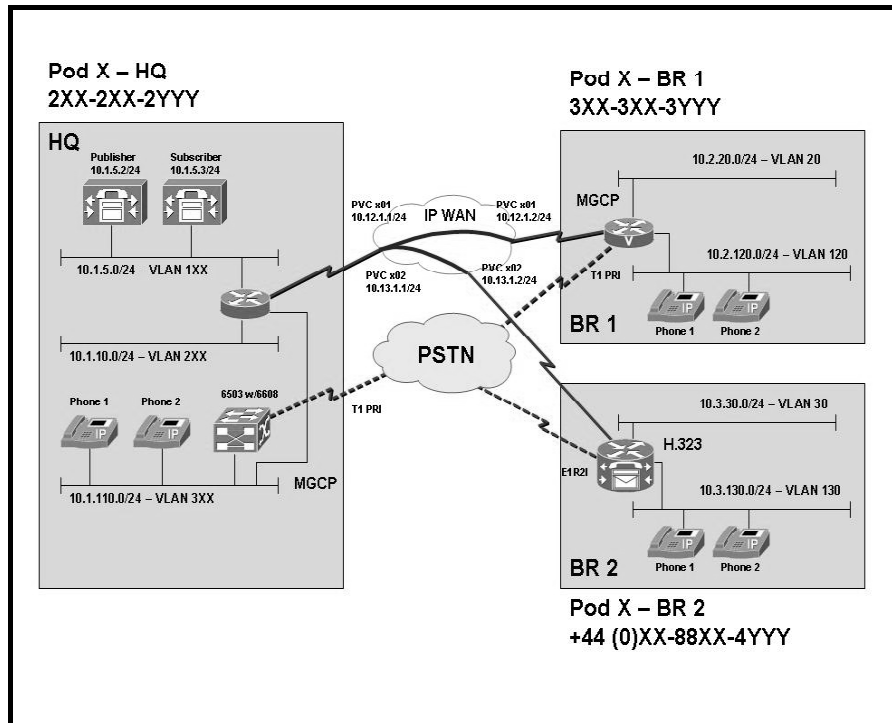
Activity Objective

In this activity, you will configure the PSTN connections in the Armstrong Snow Shovel network. After completing this activity, you will be able to meet these objectives:

- Configure a PRI network connection
- Configure a CAS network connection

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Student Pods

The student pod equipment requirements are as follows:

- Six Cisco IP Phones, which can be any model except for 7920. The IP Phones require power from either an in-line power switch or external power bricks.
- One Cisco router with one 10/100 Ethernet interface, one T1 serial interface, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one T1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one E1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco Catalyst 3550 switch for each branch location or one internal EtherSwitch module for the router.
- One Cisco Catalyst 6500 switch, one 10/100 Ethernet switch module, and one WS-X6608 gateway module for the HQ location.
- One Cisco CallManager publisher and one subscriber.

Network Core

The network core equipment requirements are as follows:

- One Cisco router to provide Frame Relay or ATM support to an IP WAN to connect the HQ with BR1 and BR2.
- One Cisco CallManager and one Cisco router configured as an MGCP gateway to provide the functionality of the PSTN to all locations.

Command List

The table describes the commands that are used in this activity.

Circuit Commands

Command	Description
<code>codec {<i>codec</i> [bytes <i>payload_size</i>] transparent}</code>	<p>This command has these keywords and arguments:</p> <ul style="list-style-type: none">■ <i>codec</i>—Codec options available for the various platforms■ bytes—(Optional) Specifies the number of bytes in the voice payload of each frame■ <i>payload-size</i>—(Optional) Number of bytes in the voice payload of each frame■ transparent—Enables codec capabilities to be passed transparently between endpoints in a Cisco Multiservice IP-to-IP Gateway

Command	Description
	Note: The transparent keyword is available only on the Cisco 2600 and 3600 Series routers and the Cisco 7200 and 7500 Series router platforms.
<code>configure terminal</code>	Enters configuration mode
<code>controller {t1 e1 j1} slot/port number</code>	<p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ t1—T1 controller. ■ e1—E1 controller. ■ j1—J1 controller. ■ <i>slot/port</i>—Backplane slot number and port number on the interface. Refer to your hardware installation manual for the specific values and slot numbers. ■ <i>number</i>— NPM number, in the range of 0 through 2.
<code>destination-pattern [+] string [T]</code>	<p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ +—(Optional) Character that indicates an E.164 standard number. ■ <i>string</i>—Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and these special characters: <ul style="list-style-type: none"> — The 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 (this character is used as a wildcard). — Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. — Plus sign (+), which indicates that the preceding digit occurred one or more times. <p>Note: The plus sign that is used as part of a digit string is different from the plus sign that can be used in front of a digit string to indicate that the string is an E.164 standard number.</p> <ul style="list-style-type: none"> — Circumflex (^), which indicates a match to the beginning of the string. — Dollar sign (\$), which matches the null string at the end of the input string. — Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). — Question mark (?), which indicates that the preceding digit occurred zero or one time. — Brackets ([]), which indicate a range. A range is a sequence of characters, which are enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range.

Command	Description
	<ul style="list-style-type: none"> — Parentheses (()), which indicate a pattern and are the same as the regular expression rule. — T—(Optional) Control character that indicates that the destination-pattern value is a variable-length dial string.
<pre>dial-peer voice tag {pots voatm vofr voip}</pre>	<p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ tag—Digits that define a particular dial peer. The range is from 1 to 2147483647. ■ pots—Indicates that this is a POTS peer that uses VoIP encapsulation on the IP backbone. ■ voatm—Specifies that this is a VoATM dial peer that uses real-time AAL5 voice encapsulation on the ATM backbone network. ■ vofr—Specifies that this is a VoFR dial peer that uses FRF.11 encapsulation on the Frame Relay backbone network. ■ voip—Indicates that this is a VoIP peer that uses voice encapsulation on the POTS network.
<pre>dial-peer voice tag type incoming called-number destination-pattern direct-inward-dial port prefix</pre>	<p>Specifies, for each POTS peer, these elements: incoming called number, destination pattern, and direct inward dial.</p>
<pre>direct-inward-dial</pre>	<p>To enable the DID call treatment for an incoming called number, use the direct-inward-dial command in dial-peer configuration mode. To disable DID on the dial peer, use the no form of this command.</p> <p>This command has no arguments or keywords.</p>
<pre>ds0-group group-number timeslots range type type {dtmf mf} {ani dnis ani-dnis}</pre>	<p>Configures all channels for E&M, FXS, and SAS analog signaling. The T1 range is from 1 to 24. The E1 range is from 1 to 31.</p> <p>Some of the valid signaling types and keyword combinations are as follows:</p> <ul style="list-style-type: none"> ■ Type: e&m-fgb: <ul style="list-style-type: none"> — dtmf and dnis — mf and dnis ■ Type: e&m-fgd: <ul style="list-style-type: none"> — dtmf and dnis — mf and ani-dnis or dnis ■ Type: fgd-eana: <ul style="list-style-type: none"> — mf and ani-dnis

Command	Description
<code>dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal] [rtp-nte]</code>	<p>This command has these keywords:</p> <ul style="list-style-type: none"> ■ cisco-rtp—(Optional) Forwards DTMF tones by using RTP with a Cisco proprietary payload type. ■ h245-alphanumeric—(Optional) Forwards DTMF tones by using the H.245 “alphanumeric” UUI method. Supports tones from 0 to 9, *, #, and from A to D. ■ h245-signal—(Optional) Forwards DTMF tones by using the H.245 “signal” UUI method. Supports tones from 0 to 9, *, #, and from A to D. ■ rtp-nte—(Optional) Forwards DTMF tones by using RTP with the NTE payload type.
<code>enable</code>	Enters privileged EXEC mode. Enter your password when prompted.
<code>framing type</code>	<p>This command has these keywords:</p> <ul style="list-style-type: none"> ■ sf—Specifies super frame as the T1 frame type. This is the default. ■ esf—Specifies extended super frame as the T1 frame type. ■ crc4—Specifies CRC4 frame as the E1 frame type. This is the default for Australia. ■ no-crc4—Specifies no CRC4 frame as the E1 frame type. ■ australia—(Optional) Specifies the E1 frame type that is used in Australia.
<code>isdn-bchan-number-order {ascending descending}</code>	<p>Configures an ISDN PRI interface to make outgoing call selection in ascending or descending order—that is, to select the lowest or highest available B channel starting at either channel B1 (ascending) or channel B23 for a T1 and channel B30 for an E1 (descending). The default is descending.</p> <p>Note: Before configuring ISDN PRI on your router, check with your service vendor to determine if ISDN trunk call selection is configured for ascending or descending order. A mismatch between router and switch causes the switch to send an error message that states that the channel is not available.</p>
<code>isdn bind-13 ccm-manager</code>	To bind Layer 3 of the ISDN PRI interface of the MGCP voice gateway to the Cisco CallManager for PRI Q.931 signaling backhaul support, use the isdn bind-13 ccm-manager command in interface configuration mode. To disable this binding, use the no form of this command.
<code>isdn switch-type switch-type</code>	<p>The command has this argument:</p> <ul style="list-style-type: none"> ■ switch-type—Here are the various switch types: <ul style="list-style-type: none"> — primary-qsig—Supports QSIG signaling per Q.931. Network-side functionality is assigned with the isdn protocol-emulate command. — primary-net5—NET5 ISDN PRI switch types for Asia, Australia, and New Zealand; ETSI-compliant switches for Euro-ISDN E-DSS1 signaling system.

Command	Description
	<ul style="list-style-type: none"> — primary-ntt—Japanese ISDN PRI switch. — primary-4ess—AT&T 4ESS switch type for the United States. — primary-5ess—AT&T 5ESS switch type for the United States. — primary-dms100—NT DMS-100 switch type for the United States. — primary-ni—National ISDN switch type. — none—No switch defined.
<pre>linecode {ami b8zs hdb3}</pre>	<p>This command has these keywords:</p> <ul style="list-style-type: none"> ■ ami—Specifies AMI as the line-code type. Valid for T1 or E1 controllers. This is the default for T1 lines. ■ b8zs—Specifies B8ZS as the line-code type. Valid for T1 controller only. ■ hdb3—Specifies HDB3 as the line-code type. Valid for E1 controller only. This is the default for E1 lines.
<pre>port (dial-peer)</pre> <p>For Cisco 1750 and Cisco 3700 Series:</p> <pre>port slot-number/port</pre> <p>For Cisco 2600 Series, Cisco 3600 Series, and Cisco 7200 Series:</p> <pre>port {slot-number/subunit-number/port slot/port:ds0-group-no}</pre>	<p>This command has these arguments:</p> <ul style="list-style-type: none"> ■ <i>slot-number</i>—Number of the slot in the router in which the VIC is installed. Valid entries are from 0 to 2, depending on the slot in which it has been installed. ■ <i>port</i>—Voice port number. Valid entries are 0 and 1. ■ <i>subunit-number</i>—Subunit on the VIC in which the voice port is located. Valid entries are 0 and 1. ■ <i>slot</i>—Router location in which the voice port adapter is installed. Valid entries are 0 and 3. ■ <i>ds0-group-no</i>—Specifies the DS0 group number. Each defined DS0 group number is represented on a separate voice port. This feature allows you to define individual DS0s on the digital T1 or E1 card.
<pre>preference value</pre>	<p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>value</i>—Integer from 0 to 10, where the lower the number, the higher the preference. The default value is 0 (highest preference).
<pre>pri-group timeslots timeslot-range [nfas_d {backup none primary {nfas_int number nfas_group number rlm- group number}} service]</pre>	<p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ <i>timeslot-range</i>—A value or range of values for time slots on a T1 or E1 controller that consists of an ISDN PRI group. Use a hyphen to indicate a range. <p>Note: Groups of time slot ranges that are separated by commas (1-4,8-23, for example) are also accepted.</p> <ul style="list-style-type: none"> ■ nfas_d {backup none primary}—(Optional) Configures the operation of the ISDN PRI D channel. ■ backup—The D-channel time slot is used as the NFAS D backup. ■ none—The D-channel time slot is used as an additional B channel.

Command	Description
	<ul style="list-style-type: none"> ■ primary—The D-channel time slot is used as the NFAS D primary. The primary keyword requires further interface and group configuration: primary {nfas_int number nfas_group number rlm-group number} <ul style="list-style-type: none"> — nfas_int number—Specifies the provisioned NFAS interface as a value; the value is a number from 0 to 8. — nfas_group number—Specifies the NFAS group. — rlm-group number—Specifies the RLM group and releases the ISDN PRI signaling channel. ■ service—(Optional) Configures the service type <i>mgcp</i> for MGCP service.
<pre>sequence-numbers</pre>	<p>To enable the generation of sequence numbers in each frame that is generated by the DSP for VoFR applications, use the sequence-numbers command in dial-peer configuration mode. To disable the generation of sequence numbers, use the no form of this command.</p> <p>This command has no arguments or keywords.</p>
<pre>session protocol {aal2-trunk cisco sipv2 smtp}</pre>	<p>This command has these keywords:</p> <ul style="list-style-type: none"> ■ aal2-trunk—Dial peer uses the AAL2 nonswitched trunk session protocol. ■ cisco—Dial peer uses the proprietary Cisco VoIP session protocol. ■ sipv2—Dial peer uses the IETF SIP. Use this keyword with the SIP option. ■ smtp—Dial peer uses the SMTP session protocol.
<p>For Cisco 1751, Cisco 3725, Cisco 3745, and Cisco AS5300:</p> <pre>session target {ipv4:destination-address dns:[\$\$\$. \$d\$. \$e\$. \$u\$.] host-name enum:table-num loopback:rtp ras sip-server}</pre> <p>For Cisco 2600 Series, Cisco 3600 Series, Cisco AS5350, Cisco AS5400, Cisco AS5850, and Cisco MC3810:</p> <pre>session target {ipv4:destination-address dns:[\$\$\$. \$d\$. \$e\$. \$u\$.] host-name enum:table-num loopback:rtp ras settlement provider-number sip-server}</pre>	<p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ ipv4:destination-address—IP address of the dial peer to receive calls. ■ dns:[\$\$\$. \$d\$. \$e\$. \$u\$.] host-name—Host device that houses the domain name server that resolves the name of the dial peer to receive calls. <p>Use one of these macros with this keyword when defining the session target for VoIP peers:</p> <ul style="list-style-type: none"> — \$\$\$.—(Optional) The source destination pattern is used as part of the domain name. — \$d\$.—(Optional) The destination number is used as part of the domain name. — \$e\$.—(Optional) The digits in the called number are reversed, and periods are added between the digits of the called number. The resulting string is used as part of the domain name. — \$u\$.—(Optional) The unmatched portion of the destination pattern (such as a defined extension number) is used as part of the domain name.

Command	Description
	<ul style="list-style-type: none"> ■ host-name—String that contains the complete host name to be associated with the target address; for example, serverA.mycompany.com. ■ enum:table-num—ENUM search table number. Range is from 1 to 15. ■ loopback:rtp—All voice data is looped back to the source. ■ ras—The RAS signaling function protocol is being used, which means that a gatekeeper is consulted to translate the E.164 address into an IP address. ■ settlement provider-number—The settlement server is the target to resolve the terminating gateway address. The argument is as follows: <ul style="list-style-type: none"> — <i>provider-number</i>—Provider IP address. ■ sip-server—The global SIP server is the destination for calls from this dial peer.
<pre>show controllers e1 [slot/port]</pre>	<p>To display information about E1 links, use the show controllers e1 command in privileged EXEC mode.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ slot/port—(Optional) Backplane slot number and port number on the interface. Refer to the hardware manuals for your controller type to determine specific slot and port numbers.
<pre>show controllers t1 [slot/port] [bert]</pre>	<p>To display information about the T1 links and to display the hardware and software driver information for the T1 controller, use the show controllers t1 command in privileged EXEC mode.</p> <p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ slot/port—(Optional) Backplane slot number and port number on the interface. Refer to your hardware installation manual for the specific slot and port numbers. ■ bert—(Optional) Type bert to get a specific display for the BERT results. Otherwise, the display will include all other non-BERT information.
<pre>show isdn {active [dsl serial-number] history [dsl serial-number] memory service [dsl serial-number] status [dsl serial-number] timers [dsl serial- number]}</pre>	<p>To display the information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels, use the show isdn command in EXEC mode.</p> <p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ active [dsl serial-number]—Displays current call information for all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range from 0 to 15. The information that is displayed includes the called number, the remote node name, the seconds of connect time, the seconds of connect time that are remaining, the seconds idle, and the AOC charging time units that are used during the call.

Command	Description
	<ul style="list-style-type: none"> ■ history [<i>dsl</i> <i>serial-number</i>] —Displays historic and current call information for all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range from 0 to 15. The information that is displayed includes the called number, the remote node name, the seconds of connect time, the seconds of connect time that are remaining, the seconds idle, and the AOC charging time units that are used during the call. ■ memory —Displays ISDN memory pool statistics. This keyword is for use by technical development staff only. ■ service [<i>dsl</i> <i>serial-number</i>] —Displays the service status of all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range from 0 to 15. ■ status [<i>dsl</i> <i>serial-number</i>] —Displays the status of all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range from 0 to 15. ■ timers [<i>dsl</i> <i>serial-number</i>] —Displays the values of Layer 2 and Layer 3 timers for all ISDN interfaces or, optionally, a specific DSL or a specific ISDN PRI interface (created and configured as a serial interface). Values of <i>dsl</i> range from 0 to 15.
<pre>show voice port [slot/subunit/port summary] For Cisco 2600 and Cisco 3600 Series routers with digital voice ports (with T1 packet voice trunk network modules): show voice port [slot/port:ds0-group summary]</pre>	<p>Use this command to display configuration and VIC information about a specific port.</p> <p>This command applies to VoIP, VoFR, and VoATM.</p> <p>The ds0-group command automatically creates a logical voice port that is numbered as follows on Cisco 2600, 3600, and 7200 Series routers: <i>slot/port:ds0-group-no</i>. Although only one voice port is created for each group, applicable calls are routed to any channel in the group.</p>

Job Aids

There are no job aids for this lab activity.

Task 1: Configure a PRI Connection to the PSTN

The HQ location for Armstrong Snow Shovel has in place today a PRI connection to the PSTN. Because this is the HQ location, all of the time slots will be used for voice. The carrier uses the NI switch type with ESF and B8ZS. The PSTN carrier provides clocking.

Activity Procedure

Complete these steps:

- Step 1** Verify that the PRI connection at HQ to the PSTN is set up correctly on port 2/1.
- Step 2** Configure the BR1 router to use a T1 PRI to connect to the PSTN. The switch type is NI, and the carrier provides clocking. The framing and line code are the same as for the HQ location. Provide support for six simultaneous calls.

Activity Verification

You have completed this task when you attain these results:

- You can verify that there is a connection to the PSTN through the PRI. Use the appropriate **show** and **debug** commands to verify the connection.

Task 2: Configure an E1R2 CAS Connection at Branch 2

Site 2 will use an E1R2 CAS connection to the PSTN.

Activity Procedure

Complete this step:

- Step 1** Provision the interface to support four simultaneous calls and to support DNIS. Use the default line code for this interface and ITU Q941 digital signaling and DTMF register signaling. .

Activity Verification

You have completed this task when you attain these results:

- You can use the appropriate **show** and **debug** commands to verify the E1R2 CAS connection to the PSTN

Lab 2-1 Answer Key: Configuring PSTN Connections

When you complete this activity, your configuration will be similar to the results here, with differences that are specific to your device or workgroup:

Configuration Steps

Step 1 Verify HQ gateway registration in Cisco CallManager device or gateway menu.

Step 2 Type these commands in BR1:

```
isdn switch-type primary-ni
controller t1 1/0
framing esf
linecode b8zs
pri-group timeslots 1-6 service mgcp
interface serial 1/0:23
isdn bind-13 ccm-manager
```

Step 3 Type these commands in BR2:

```
controller e1 1/0
ds0-group 1 timeslots 1-4 type r2-digital dtmf dnis
```


Case Study 2-2: Migrating to IP Telephony from a PBX-Based System

This case study allows you to practice the skills and knowledge learned in the module.

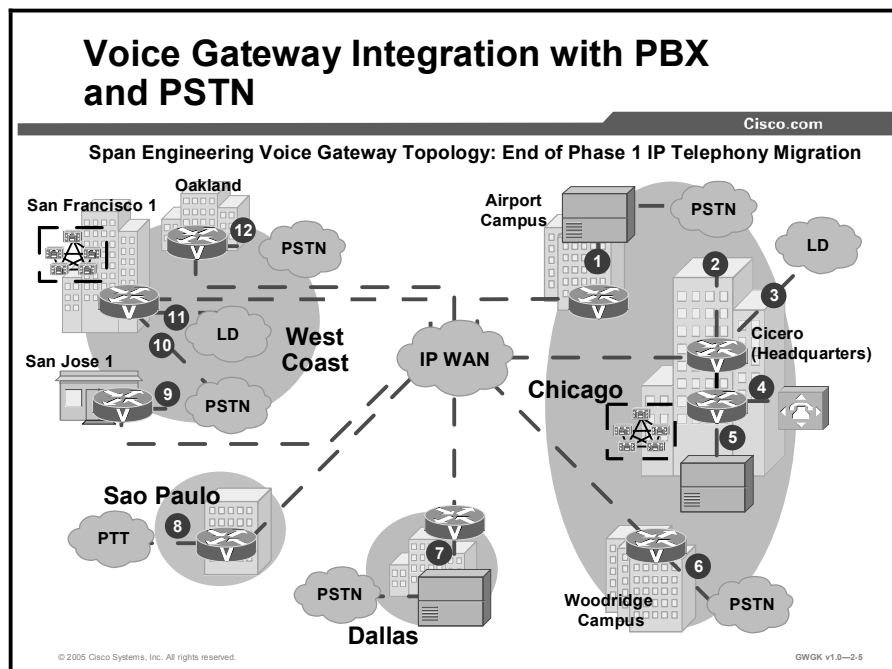
Activity Objective

In this activity, you are given deployment requirements. You will describe the procedure for, and underlying issues of, connecting voice gateways to PBXs. After completing this activity, you will be able to meet these objectives:

- Explain the issues that may occur when you are connecting a voice gateway to a PBX while trying to maintain a given set of telephony features
- Show on a topology diagram that the best ends of given PRI connections are the network and user sides
- Explain where multiple PRIs derive their clocking from
- Create a list of tasks to do in order to connect a voice gateway to a PBX

Visual Objective

The figure illustrates what you will accomplish in this activity. You will describe voice-gateway-to-PBX integration issues for connections 1, 2, and 3.



Required Resources

These are the resources that are required to complete this activity:

- Use the scenarios, information, and parameters that are provided at each task of an ongoing case study. If there are ambiguities, make reasonable assumptions and proceed. For all the tasks, use the initial customer scenario and build on the solutions that you have developed so far.
- You may use all documentation, books, white papers, and so on that are available.
- You may use the Cisco Interoperability Portal at http://www.cisco.com/warp/public/779/largeent/avid/inter_operability/.
- In each task of the case study, you will work with a partner and together act as a network administrator. Make creative proposals to help the enterprise accomplish its goals. When your ideas differ from those of the instructor, justify your ideas.
- Use any implementation strategies that you feel are appropriate.
- A final goal for each case study is a whiteboard solution.

The PBX and PSTN Integration Problem

In this case study you are given a scenario in which an organization is carrying out a staged migration of its telephony infrastructure to IP telephony. Acting in the role of a member of the team responsible for the migration, you and a partner will prepare notes on issues and tasks that are related to the connection of a voice gateway to a PBX.

This activity includes these tasks:

- Task 1: “Analyzing Issues for Airport Campus Toll Bypass.” This task involves the connection of analog and T1 CAS trunks between a voice gateway and a PBX. What are the challenges that are involved with maintaining existing services through the gateway over these trunks?
- Task 2: “Analyzing Issues for Cicero Campus IP Telephony Migration.” This task involves the connection of QSIG PRIs between a voice gateway and a PBX. What are the issues that must be considered with these connections to ensure that the service functions as users expect?

Task 1: Analyze Issues for Airport Campus Toll Bypass

This task asks you to consider issues with analog and T1 CAS trunks.

Read and discuss this scenario. Allow 5 to 10 minutes to completely read the scenario. Take 10 minutes to discuss with your partner the scenario and the questions that are listed in the accompanying steps. You may refer to the Cisco Interoperability Portal, the references that are provided by your instructor, or any other resource that is available to you in the classroom or online.

Company Facts

Span Engineering is a U.S. company with headquarters in Chicago. It has branches in Dallas and on the West Coast in the California Bay Area, and has recently expanded internationally to São Paulo, Brazil. The company is carrying out a phased migration to IP telephony:

- **Phase 1:** Toll bypass between Dallas and Chicago and between Chicago area campuses.
- **Phase 2:** Migration Stage 1. Span Engineering deploys Cisco CallManager in Chicago, the West Coast, Dallas, and São Paulo. Some locations have migrated to IP telephony, and some remain on PBX as shown in Case Study Figure 1. This will be done immediately following toll bypass implementation. This phase is applicable to Task 2 of this case study.

The voice gateway topology of the Span Engineering migration after Phase 2 is shown in the previous visual objective figure. The trunks, which are numbered 1, 2, and 3 in the visual objective, are described in the table here.

IP Telephony Design Connections for PBX and PSTN Integration

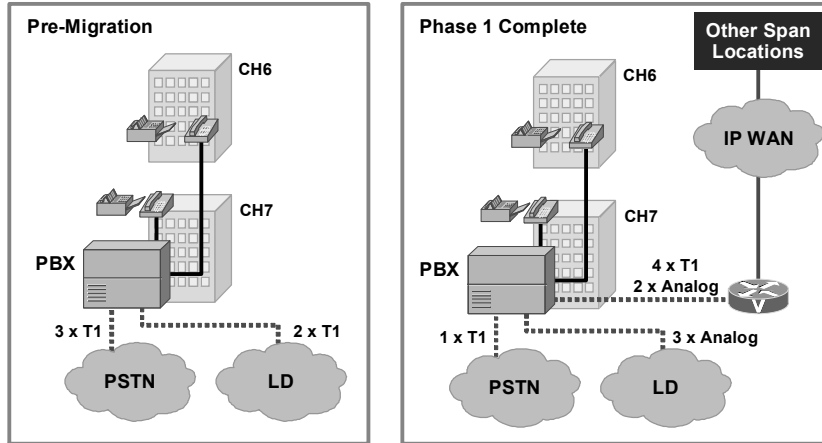
Connection	Connects Gateway to	Description	Gateway Recommended by Designer
1	Nortel Meridian Opt 11c	4 x T1 CAS 2 x Analog	2 x VWIC-2MFT-T1 in a 2811
2	Nortel Meridian 1 Release 25	4 x T1 PRI	NM-2CT1 in a 3825
3	Avaya MV1.3 PBX	2 x T1 PRI	VWIC-1MFT-T1 in a 3825

The Span Engineering facility near the Chicago airport has two buildings that are served by an old analog PBX. The Phase 1 plan for the airport is to provide toll bypass.

Span Engineering Chicago—Airport Campus

Cisco.com

Topology before and after toll bypass implementation



© 2005 Cisco Systems, Inc. All rights reserved.

GWGK v1.0-2.3

Case Study Figure 1 Scenario at the Airport Campus Before and After Phase 1

The two tables that follow contain information that you have extracted from the IP telephony design and from some information that you had on file regarding the airport campus.

Trunks at the Span Engineering Airport Campus

Migration Phase	Type of Traffic	Trunks
Existing trunks (premigration)	Premigration total	3 x T1 CAS to local PSTN 2 x T1 CAS to long-distance
	End Phase 1—postmigration to toll bypass	4 x T1 CAS 2 x analog lines
	Local PSTN	1 x T1 CAS
	Long-distance	3 x analog lines

Phone Features by User Group

User Group	Number in Group	Premigration Phone Features
Management and Administration	20	Caller ID Hold DND Call Park Call Transfer Callback Call Forward Three-way conference calling Voice mail
Standard	325	Hold Call Park Call Transfer Voice mail

With a partner, discuss the connection between the PBX and the voice gateway. Consider any challenges that may arise in ensuring that users continue to get the features that they have now. Also devise a step-by-step procedure that you can follow to carry out the implementation of the connection between the gateway and the PBX. Use the task steps that follow and the Case Study Task 1 Response Form to guide your discussion.

Complete these steps:

- Step 1** Review the existing phone features that are described in the table “Phone Features by User Group.” Explain how these features can be maintained through the voice gateway for toll bypass calls. What issues do you anticipate for the continued provision of these features with the analog lines that are identified by the designer? What about the T1 CAS trunks?
- Step 2** What steps will you follow to connect the gateway to the PBX?

Case Study Task 1 Response Form

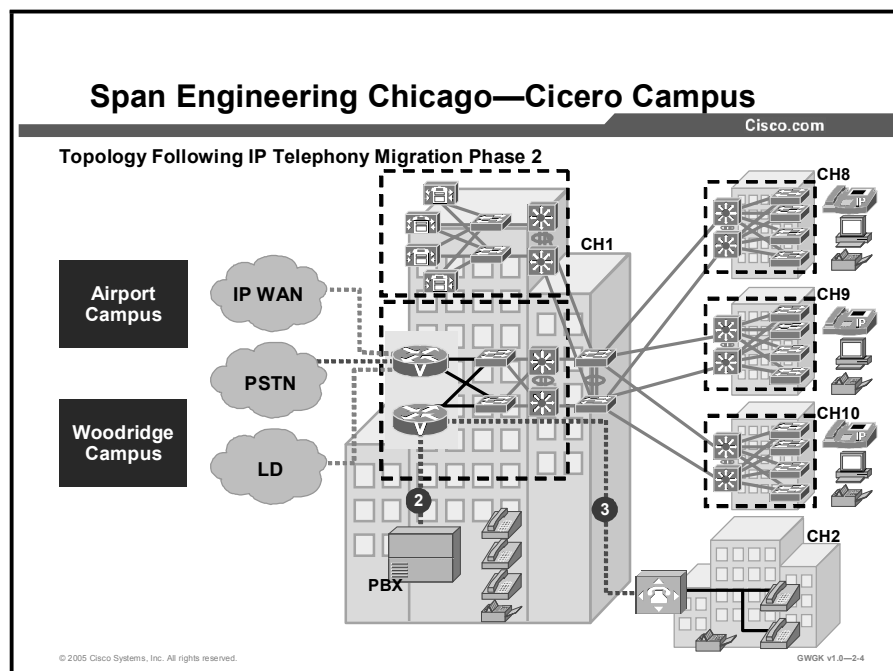
Step	Requirement	Proposed Solution
1.	<p>What considerations are there with respect to the different features that are assigned to the two different user groups?</p> <p>(Use a blank page for overflow text.)</p>	
	<p>Explain how support for features will be provided on the analog lines.</p> <p>(Use a blank page for overflow text.)</p>	
	<p>Explain how support for features will be provided over T1 CAS.</p> <p>(Use a blank page for overflow text.)</p>	
2.	<p>List the steps that you will follow to connect the voice gateway to the PBX.</p> <p>(Use a blank page for overflow text.)</p>	

Task 2: Analyze Issues for Cicero Campus IP Telephony Migration

Read and discuss this scenario. Allow 5 to 10 minutes to completely read the scenario. Take 20 minutes to discuss with your partner the scenario and the questions that are listed in the accompanying steps. You may refer to the Cisco Interoperability Portal, the references that are provided by your instructor, or any other resource that is available to you in the classroom or online.

Update to the Company Situation

The Span Engineering Cicero campus has five buildings: a headquarters building, an administration building, and three buildings for engineering operations. As part of Phase 2 of the Span Engineering migration plan, the engineering operations buildings will be receiving IP telephony.



Case Study Figure 2 Scenario at the Cicero Campus After Phase 2

An excerpt from the connections table from the scenario is reproduced here for easy cross-referencing with the figure.

Span Engineering LLC Connections for PBX and PSTN Integration

Connection	Connects Gateway to	Description	Gateway Recommended by Designer
2	Nortel Meridian 1 Release 25	4 x T1 PRI QSIG	NM-2CT1 in a 3825
3	Avaya MV1.3 PBX	2 x T1 PRI	VVIC-1MFT-T1 in a 3825

The two tables that follow contain information that you have extracted from the IP telephony design and from some information that you had on file regarding the airport campus.

Phone Features by User Group

User Group	Number in Group	Premigration Phone Features
Standard	700	Hold Call Park Call Transfer Voice mail
Management and Administration (Engineers and technicians get same privileges.)	1,400	As for the standard user group plus: Caller ID DND Callback Call Forward Three-way conference calling
Executive and EA	53	As for the management and administration user group plus: Call Barge

Similar to Task 1, with a partner, discuss the connections between the PBX and the voice gateways and consider any challenges that may arise in ensuring that users continue to get the telephony service that they have now. Use the task steps that follow and the Case Study Task 2 Response Form to guide your discussion.

Note Fax and E911 service will be provided through a Cisco VG248 gateway that is not shown. The existing voice-mail solution will be maintained.

Complete these steps:

- Step 1** For connections 2, and 3, in Case Study Figure 2, show which is the network side and which is the user side of each connection. Explain what possible problems might occur if this is not identified for a trunk.
- Step 2** Where will connections 2 and 3 derive their clocking from? Connection 2 consists of 4 T1s. How will each of the individual T1s be clocked?
- Step 3** From the Cisco Interoperability Portal, find a document that most closely resembles the scenario for connection 2. Using that document, create a list of things to consider prior to configuring the gateway-to-PBX connection. What are the issues that you are most concerned with that may generate trouble calls from users with this connection? What would your plan, or task sequence, be for making connection 2 if you really had to do it?

Case Study Task 2 Response Form

Step	Requirement	Proposed Solution
1.	Provide a topology diagram for connections 2 and 3 showing which side should be the network side and which should be the user side for each connection. Explain the issues that might arise if a network side is not identified.	Do the sketch on Figure 2. This is class instructed case study. The sketch is a drawing of the gateway to PSTN topology. The students will know what to do. Explain the issues here.
2.	Explain where connections 2 and 3 get their clocking from and how each PRI on connection 2 is clocked.	
3.	Connect a voice gateway to a PBX for connection 2.	<p>Title of document that is selected from Cisco Interoperability Portal:</p> <p>Limitations that are listed in the document:</p> <p>Impact that these limitations have on connection 2:</p> <p>Given the current user features, the type of PBX, and the type of trunk, what preconfiguration considerations will you observe?</p> <p>What steps will you take to complete the connection?</p>

Activity Verification

You have completed this activity when the instructor has verified your case study solution and you have justified any major deviations from the case study solution that is supplied by the instructor.

Case Study 2-2 Answer Key: Migrating to IP Telephony from a PBX-Based System

Your case study discussion and solution should include these items:

- A completed Task 1 Response Form that includes these items:
 - An explanation of how support for features will be provided on the analog lines
 - An explanation of how support for features will be provided over T1 CAS
 - A list of the steps that you will follow to connect the voice gateway to the PBX
- A completed Task 2 Response Form that includes these items:
 - Identification of the network side and the user side of the two given connections in Figure 2
 - An explanation of where the various trunks derive their clocking from
 - Considerations for sustaining the services and features that users expect once the voice gateway has been inserted into telephony topology of the company
 - A list of the steps that you will follow to connect the PRI QSIG trunks from the PBX to the voice gateway

Lab 3-1: Implementing a Dial Plan and COR

Complete this lab activity to practice what you learned in the related module.

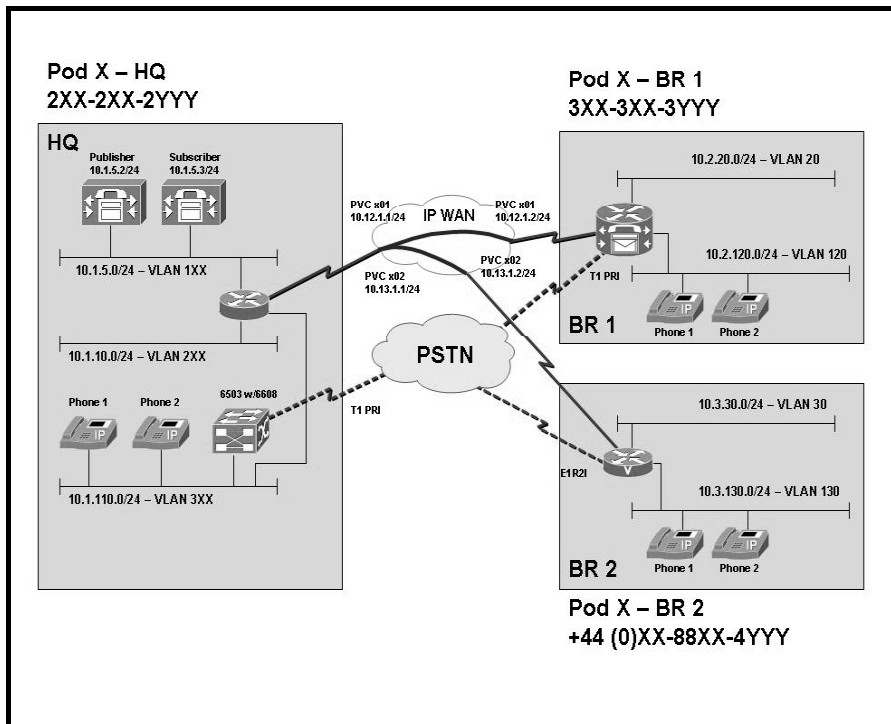
Activity Objective

In this activity, you will configure dial peers so that dialing four digits will allow calls to be placed from extension to extension across the IP WAN. You will also implement CoS for Branch 2. After completing this activity, you will be able to meet these objectives:

- Deploy a dial plan at BR2
- Deploy COR at BR2

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Student Pods

The student pod equipment requirements are as follows:

- Six Cisco IP Phones, which can be any model except for 7920. The IP Phones require power from either an in-line power switch or external power bricks.
- One Cisco router with one 10/100 Ethernet interface, one T1 serial interface, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one T1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one E1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco Catalyst 3550 switch for each branch location or one internal EtherSwitch module for the router.
- One Cisco Catalyst 6500 switch with a 10/100 Ethernet switch module and a WS-X6608 gateway module for the HQ location.
- One Cisco CallManager publisher and subscriber.

Network Core

The network core equipment requirements are as follows:

- One Cisco router to provide Frame Relay or ATM support to an IP WAN to connect the HQ with BR1 and BR2.
- One Cisco CallManager and one Cisco router that are configured as an MGCP gateway to provide the functionality of the PSTN to all locations.

Command List

The table describes the commands that are used in this activity.

Voice Configuration Commands

Command	Description
<code>answer-address string</code>	(Optional) Selects the inbound dial peer based on the calling number.
<code>codec {g711alaw g711ulaw g723ar53 g723ar63 g723r53 g723r63 g726r16 g726r24 g726r32 g728 g729br8 g729r8 [pre-ietf]} [bytes]</code>	<p>Defines the codec for the dial peer.</p> <p>The optional <i>bytes</i> parameter sets the number of voice data bytes per frame. Acceptable values are from 10 to 240 in increments of 10 (for example, 10, 20, 30, and so on). Any other value is rounded down (for example, from 236 to 230).</p> <p>The same codec value must be configured in both VoIP dial peers on either side of the connection.</p> <p>If you specify g729r8, then IETF bit ordering is used. For interoperability with a Cisco 2600 Series, Cisco 3600 Series, or Cisco AS5300 gateway that is operating a release earlier than Cisco IOS Release 12.0(5)T or 12.0(4)XH, you <i>must</i> specify the additional keyword pre-ietf after g729r8.</p> <p>The codec command syntax is platform- and release-specific. For more information about the syntax of this command, refer to the <i>Cisco IOS Voice, Video, and Fax Command Reference</i>.</p>
<code>corlist incoming cor-list-name</code>	<p>To specify the COR list that is to be used when a specified dial peer acts as the incoming dial peer, use the corlist incoming command in dial-peer configuration mode. To clear the previously defined incoming COR list in preparation for redefining the incoming COR list, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>cor-list-name</i>—Name of the dial-peer COR list that defines the capabilities that the specified dial peer has when it is used as an incoming dial peer.
<code>corlist outgoing cor-list-name</code>	<p>To specify the COR list to be used by outgoing dial peers, use the corlist outgoing command in dial-peer configuration mode. To clear the previously defined outgoing COR list in preparation for redefining the outgoing COR list, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>cor-list-name</i>—Required name of the dial-peer COR list for outgoing calls to the configured number that is using this dial peer.
<code>dial-peer cor custom</code>	Enters COR configuration mode to specify classes of restrictions to apply to dial peers.
<code>dial-peer corlist list-name</code>	Provides a name for a list of restrictions.
<code>dial-peer voice number pots</code>	Enters dial-peer configuration mode and defines a local dial peer that connects to a POTS interface.

Command	Description
	<p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ <i>number</i>—This argument is one or more digits that identify the dial peer. Valid entries are from 1 to 2147483647. ■ pots—This keyword indicates a dial peer that is using basic telephone service.
dial-peer voice <i>number</i> voip	<p>Enters dial-peer configuration mode and defines a remote VoIP dial peer.</p> <p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ <i>number</i>—This argument is one or more digits that identify the dial peer. Valid entries are from 1 to 2147483647. ■ voip—This keyword indicates a dial peer that is using voice encapsulation on the IP network.
destination-pattern <i>string</i> [T]	<p>Configures the dial-peer destination pattern so that the system can reconcile dialed digits with a telephone number.</p> <p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ <i>string</i>—This argument is a series of digits that specify the E.164 or private dialing plan telephone number. Valid entries are the numbers 0 through 9 and the letters A through D. You can also enter these special characters: <ul style="list-style-type: none"> — The asterisk (*) or pound sign (#) on standard touch-tone dial pads can be used anywhere in the pattern. — The period (.) acts as a wildcard character. ■ T—When the timer (T) character is included at the end of the destination pattern, the router collects dialed digits until the interdigit timer expires (10 seconds, by default) or until you dial the termination character (the default is #). The timer character must be a capital T.
direct-inward-dial <i>string</i>	(Optional) Enables the DID call treatment for the incoming called number.
forward-digits { <i>num-digit</i> all extra }	(Optional) Configures the digit-forwarding method that is used by the dial peer. The valid range for the number of digits that are forwarded (<i>num-digit</i>) is 0 through 32.
incoming called-number <i>string</i>	(Optional) Selects the inbound dial peer that is based on the called number to identify voice and modem calls.
max-conn <i>number</i>	(Optional) Specifies the maximum number of allowed connections to and from the POTS dial peer. The valid range is 1 through 2147483647.
member <i>class-name</i>	<p>To add a member to a dial-peer COR list, use the member command in dial-peer COR list configuration mode. To remove a member from a list, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>class-name</i>—Class name that was previously defined in dial-peer COR custom configuration mode by use of the name command.

Command	Description
name <i>class-name</i>	Provides a name for COR. Note: Repeat this step for additional class names, as needed. These class names are used to define the COR lists.
numbering-type { abbreviated international national network reserved subscriber unknown }	(Optional) Specifies the numbering type to match, as defined by the ITU Q.931 specification.
port For Cisco 1750 and Cisco 3700 Series: port <i>slot-number/port</i> no port <i>slot-number/port</i> For Cisco 2600 Series, 3600 Series, and 7200 Series: port { <i>slot-number/subunit-</i> <i>number/port</i> <i>slot/port:ds0-group-no</i> } no port { <i>slot-</i> <i>number/subunit-number/port</i> <i>slot/port:ds0-group-no</i> }	To associate a dial peer with a specific voice port, use the port command in dial-peer configuration mode. To cancel this association, use the no form of this command. This command has these arguments: <ul style="list-style-type: none">■ <i>slot-number</i>—Number of the slot in the router in which the VIC is installed. Valid entries are from 0 to 2, depending on the slot in which it has been installed.■ <i>port</i>—Voice port number. Valid entries are 0 and 1
preference <i>value</i>	(Optional) Configures a preference for the POTS dial peer. The valid range is 0 through 10, where the lower the number, the higher the preference.
prefix <i>string</i>	(Optional) Includes a prefix that the system adds automatically to the front of the dial string before passing it to the telephony interface. Valid entries for the <i>string</i> argument are 0 through 9 and a comma (.). Use a comma to include a one-second pause between digits to allow for a secondary dial tone.
rule <i>precedence /match-</i> <i>pattern/ /replace-pattern/</i> [type { <i>match-type</i> <i>replace-</i> <i>type</i> } [plan { <i>match-type</i> <i>replace-type</i> }]]	To define a translation rule, use the rule command in voice translation-rule configuration mode. To delete the translation rule, use the no form of this command. This command has these keywords and arguments: <ul style="list-style-type: none">■ <i>precedence</i>—Priority of the translation rule. Range is from 1 to 15.■ <i>/match-pattern/</i>— SED expression that is used to match incoming call information. The slash ("/") is a delimiter in the pattern.■ <i>/replace-pattern/</i>—SED expression that is used to replace the match pattern in the call information. The slash ("/") is a delimiter in the pattern. (See the next table for examples of regular expression usage.)■ type <i>match-type</i> <i>replace-type</i>—(Optional) Number type of the call. Valid values for the <i>match-type</i> argument are as follows:<ul style="list-style-type: none">— abbreviated—Abbreviated representation of the complete number as supported by this network.

Command	Description
	<ul style="list-style-type: none"> — any—Any type of called number. — international—Number that is called to reach a subscriber in another country. — national—Number that is called to reach a subscriber in the same country, but outside the local network. — network—Administrative or service number specific to the serving network. — reserved—Reserved for extension. — subscriber—Number that is called to reach a subscriber in the same local network. — unknown—Number of a type that is unknown by the network. <p>Valid values for the <i>replace-type</i> argument are as follows:</p> <ul style="list-style-type: none"> — abbreviated—Abbreviated representation of the complete number as supported by this network. — international—Number that is called to reach a subscriber in another country. — national—Number that is called to reach a subscriber in the same country, but outside the local network. — network—Administrative or service number specific to the serving network. — reserved—Reserved for extension. — subscriber—Number that is called to reach a subscriber in the same local network. — unknown—Number of a type that is unknown by the network. <ul style="list-style-type: none"> ■ plan <i>match-type replace-type</i>—(Optional) Numbering plan of the call. Valid values for the <i>match-type</i> argument are as follows: <ul style="list-style-type: none"> — any—Any type of dialed number. — data — ermes — isdn — national—Number that is called to reach a subscriber in the same country, but outside the local network. — private — reserved—Reserved for extension. — telex — unknown—Number of a type that is unknown by the network. <p>Valid values for the <i>replace-type</i> argument are as follows:</p> <ul style="list-style-type: none"> — data

Command	Description
	<ul style="list-style-type: none"> — ermes — isdn — national—Number that is called to reach a subscriber in the same country, but outside the local network. — private — reserved—Reserved for extension. — telex — unknown—Number of a type that is unknown by the network. ■ reject—The match pattern of a translation rule is used for call reject purposes.
<pre>session target { ipv4:destination-address dns:[ss\$. \$d\$. \$e\$. \$u\$.] host-name }</pre>	<p>Defines the IP address of the router that is connected to the remote telephony device.</p> <p>The ipv4:destination-address keyword and argument indicate the IP address of the remote router.</p> <p>The dns:host-name keyword and argument indicate that the DNS will resolve the name of the IP address. Valid entries for this parameter are characters that represent the name of the host device.</p> <p>Wildcards are also available for defining domain names with the keyword by using source, destination, and dialed information in the host name.</p>

Regular Expression Examples

Here is a little more information related to Regular Expressions:

- A translation rule applies to a calling party number (ANI) or a called party number (DNIS) for incoming, outgoing, and redirected calls within Cisco H.323 voice-enabled gateways.
- Number translation occurs several times during the call-routing process. In both the originating and terminating gateways, the incoming call is translated before an inbound dial peer is matched, before an outbound dial peer is matched, and before a call request is set up. Your dial plan should account for these translation steps when translation rules are defined.
- Each rule consists of SED-like expressions for the matching and replacement patterns, and may include any of these components:
 - Escape sequences using backslashes
 - Keywords “NULL” and “ANY”
 - A CTRL-V before a question mark (“?”) in order to use the question mark as a symbol in a match pattern
 - Either “&” or “\0” for copying the substring that is matched by the match pattern

The table here shows examples of match patterns, input strings, and result strings.

Match Patterns, Input Strings, and Result Strings

Match Pattern	Replacement Pattern	Input String	Result String	Description
/^\$/	//			Null string to null string.
/^.*\$/	//	4085662711		Any string to null string.
//	//	4085551234	4085551234	Match any string but no replacement. Use this to manipulate the call plan or call type.
/^456\ (.*\)/	/555\1/	4567123	5557123	Match from the beginning of the input string.
/\ (^...\)456\ (... \)/	/\1555\2/	4084567777	4085557777	Match from the middle of the input string.
/\ (.*)8920/	/\15555/	4081118920	4081115555	Match from the end of the input string.
/^1#\ (.*\)/	/\1/	1#2345	2345	Replace match string with null string.
/^408...\ (8333\)/	/555\1/	4087778333	5558333	Match multiple patterns.
/1234/	/00&00/	5551234	55500123400	Match the substring.
/1234/	/00\000/	5551234	55500123400	Match the substring (same as &).

Job Aids

These job aids are available to help you complete the lab activity.

Lab 3-1 Job Aids

Location	Dial-Plan Range
HQ	2XX-2XX-2YYY
BR1	3XX-3XX-3YYY
BR2	+44 (0) XX-88XX-4YYY

Location	Phone	Line/SD	Extension
HQ	1	Line 1	2001
	2	Line 2	2002
BR1	1	Line 1	3001
	2	Line 2	3005
BR2	1	Line 1	4001
	2	Line 1	4002
		Line 2	4006

Task 1: Deploy Dial Plan at BR2

To facilitate communications between offices of Armstrong Snow Shovel, a four-digit dialing plan has been developed. You need to implement the dial plan at BR2 to meet the requirements that are presented in the activity procedure.

Activity Procedure

Complete these steps:

- Step 1** At BR2 create a set of dial-peer statements that will support four-digit dialing to HQ and BR1.
- Step 2** Configure the gateway at BR2 so users can call emergency services and make local calls to the PSTN.

Activity Verification

You have completed this task when you can verify that the phones at BR2 can call emergency services and all other extensions at Armstrong Snow Shovel, and make local PSTN calls.

Task 2: Deploy COR

Armstrong Snow Shovel is very concerned with controlling where phone users can call. At the HQ and BR1 locations, COR is controlled by the Cisco CallManager cluster. At the BR2 location, COR needs to be configured on the Cisco CallManager Express gateway so that the users at this location have the same dialing privileges as the users at HQ and BR1.

Activity Procedure

Complete these steps:

- Step 1** Configure COR on the BR2 Cisco CallManager Express gateway. COR should be deployed in the same manner as with HQ and BR1. There are five groups of users: executives, sales administrators, engineers, administrators, and lobby and breakroom users.
- Step 2** Assign executives with unrestricted call capabilities.
- Step 3** Assign sales administrators with internal, local, and long-distance call capabilities.
- Step 4** Assign engineers with unrestricted call capabilities.
- Step 5** Assign administrators with internal and local call capabilities.
- Step 6** Assign lobby and breakroom users with internal call capabilities.

Activity Verification

You have completed this task when you can place calls to all internal and local destinations. You can verify that COR is allowing calls to be placed to the correct destinations.

Lab 3-1 Answer Key: Implementing a Dial Plan and COR

When you complete this activity, your configuration will be similar to the results here, with differences that are specific to your device or workgroup. This solution was developed on pod 8. The solution should be adjusted to match the dial plan for your assigned pod.

Task 1 Solution

Step 1 To complete Step 1 of Task 1, you must bind the H.323 gateway to an interface on the gateway. You also need to add VoIP dial peers that point to HQ and to BR1 extension ranges. Type these commands on BR2:

```
interface fastethernet0/0.30
 h323-gateway voip interface
 h323-gateway voip bind srcaddr 10.3.30.1
```

```
dial-peer voice 2000 voip
 destination-pattern 2...
 session target ipv4:10.1.5.3
```

```
dial-peer voice 3000 voip
 destination-pattern 3...
 session target ipv4:10.1.5.3
```

Step 2 To complete Step 2 of Task 1, you need to add POTS dial peers to support calls to emergency services and local dialing. The PSTN at BR2 expects local calls to begin with a 0. Type these commands on BR2:

```
dial-peer voice 911 pots
 destination-pattern 911
 prefix 911
 port 1/0:1
```

```
dial-peer voice 9911 pots
 destination-pattern 9911
 prefix 911
 port 1/0:1
```

```
dial-peer voice 9 pots
 destination-pattern 90.....
 prefix 0
 port 1/0:1
```

Task 2 Solution

Step 3

To complete Task 2, you need to build COR lists to be assigned to the outbound dial peers and COR lists that are assigned to the Cisco IP Phones under the telephony service configuration. Type these commands on BR2:

```
dial-peer cor custom
  name internal
  name emergency
  name local
  name ld

dial-peer cor list Internal
member internal

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 Lobby
member internal
member emergency

dial-peer cor list Admin
member internal
member emergency
member local

dial-peer cor list Engineer
member internal
member emergency
member local
member ld

dial-peer cor list Sales
member internal
member emergency
member local
member ld

dial-peer cor list Executive
member internal
member emergency
member local
member ld

dial-peer voice 911 pots
cor outgoing Emergency

dial-peer voice 9911 pots
cor outgoing Emergency
```



```
dial-peer voice 2000 voip
cor outgoing Internal
```

```
dial-peer voice 3000 voip
cor outgoing Internal
```

```
dial-peer voice 9 pots
cor outgoing Local
```

```
ephone-dn 1
cor incoming Engineer
```

```
ephone-dn 2
cor incoming Admin
```

```
ephone-dn 3
cor incoming Admin
```

```
ephone-dn 5
cor incoming Lobby
```

Lab 4-1: Configuring SRST

Complete this lab activity to practice what you learned in the related module.

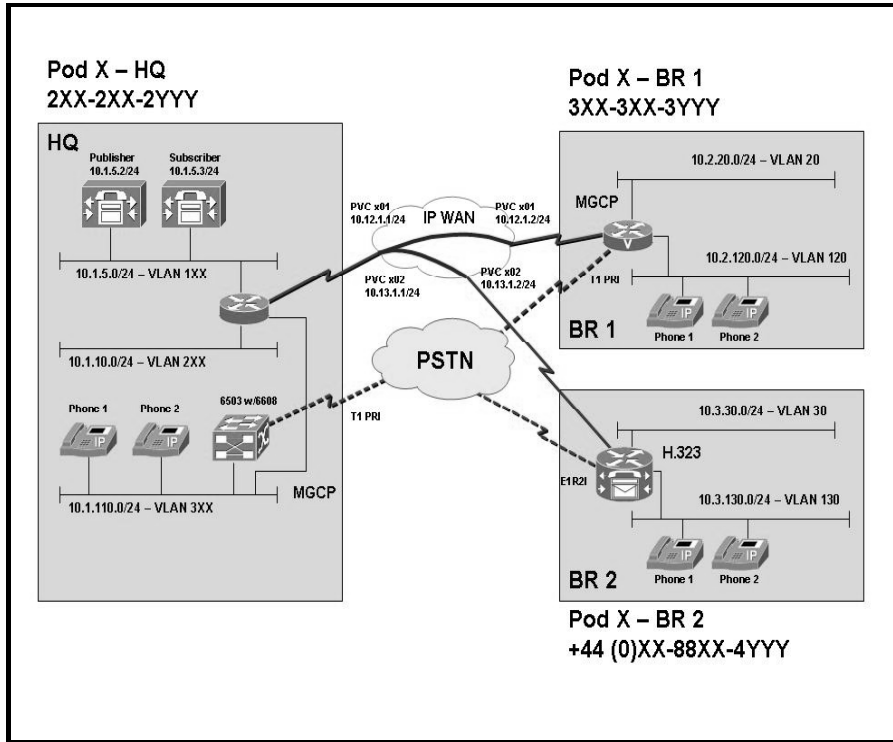
Activity Objective

In this activity, you will be able to configure a remote gateway to support SRST so that in the event of a loss of signal from the centralized Cisco CallManager cluster or an IP WAN outage, a remote facility will still have functioning Cisco IP Phones. After completing this activity, you will be able to meet these objectives:

- Configure DHCP to support SRST
- Configure SRST on a remote gateway
- Verify the operation of the remote site gateway during SRST operation

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Student Pods

The student pod equipment requirements are as follows:

- Six Cisco IP Phones, which can be any model except for 7920. The IP Phones require power from either an in-line power switch or external power bricks.
- One Cisco router with one 10/100 Ethernet interface, one T1 serial interface, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one T1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one E1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco Catalyst 3550 switch for each branch location or one internal EtherSwitch module for the router.
- One Cisco Catalyst 6500 switch with one 10/100 Ethernet switch module and one WS-X6608 gateway module for the HQ location.
- One Cisco CallManager publisher and subscriber.

Network Core

The network core equipment requirements are as follows:

- One Cisco router to provide Frame Relay or ATM support to an IP WAN to connect the HQ with BR1 and BR2.
- One Cisco CallManager and one Cisco router configured as an MGCP gateway to provide the functionality of the PSTN to all locations.

Command List

The table describes the commands that are used in this activity.

SRST Configuration Commands

Command	Description
<code>call application alternate</code> <code>[application-name]</code>	<p>To specify an alternate application to use if the application that is configured in the dial peer fails, use the call application alternate command in global configuration mode. To return to the default behavior, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none">• <i>application-name</i>—(Optional) Name of the specific voice application to use if the application in the dial peer fails. If a specific application name is not entered, the gateway uses the default application.

Command	Description
<code>call-manager-fallback</code>	To enable SRST support and enter call-manager-fallback mode, use the call-manager-fallback command in global configuration mode. To disable SRST support, use the no form of this command.
<code>ccm-manager fallback-mgcp</code>	To enable the gateway fallback feature on an MGCP voice gateway, use the ccm-manager fallback-mgcp command in global configuration mode. To disable fallback on the MGCP voice gateway, use the no form of this command.
<code>date-format {mm-dd-yy dd-mm-yy yy-dd-mm yy-mm-dd}</code>	<p>Sets the date format for Cisco IP Phone display. The choices are mm-dd-yy, dd-mm-yy, yy-dd-mm, and yy-mm-dd, where these keyword components exist</p> <ul style="list-style-type: none"> ■ dd = day ■ mm = month ■ yy = year <p>The default is set to mm-dd-yy.</p>
<code>default-router address [address2...address8]</code>	<p>Specifies the router to which the Cisco IP Phones are connected directly. This router is either a Cisco SRST router or any Cisco router that is attached to the Cisco SRST router.</p> <p>Note: As long as the Cisco IP Phones have connection to the Cisco SRST router, the Cisco IP Phones are able to get the required network details.</p> <p>The command has these arguments:</p> <ul style="list-style-type: none"> ■ address—Specifies the IP address of a router. One IP address is required, although you can specify up to eight addresses in one command line. ■ address2...address8—(Optional) Specifies up to eight addresses in the command line.
<code>exit</code>	Exits call-manager-fallback configuration mode.
<code>ip source-address ip-address [port port] [any-match strict-match]</code>	<p>To enable a router to receive messages from Cisco IP Phones through the specified IP addresses and ports, use the ip source-address command in call-manager-fallback configuration mode. To disable the router from receiving messages from Cisco IP Phones, use the no form of this command.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ ip-address—Pre-existing router IP address, typically one of the addresses of the Ethernet port of the router. ■ port—(Optional) Port to which the gateway router connects to receive messages from the Cisco IP Phones. ■ port—(Optional) Port number. The default port number is 2000. ■ any-match—(Optional) Disables strict IP address checking for registration. ■ strict-match—(Optional) Requires strict IP address checking for registration.

Command	Description
keepalive <i>seconds</i>	<p>To configure the time interval between successive keepalive messages that are sent to the router used by the Cisco IP Phones, use the keepalive command in telephony service configuration mode. To reset to the default, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ seconds—Interval time, in seconds. Range is from 10 to 65535. The default is 30.
limit-dn {7910 7935 7940 7960} <i>max-lines</i>	<p>Limits the DN lines on Cisco IP Phones during Cisco CallManager fallback.</p> <p>Note: You must configure this command during initial Cisco SRST router configuration, before any phone actually registers with the Cisco SRST router. However, you can modify the number of lines at a later time.</p> <p>The setting for maximum lines is from 1 to 6. The default number of maximum directory lines is set to 6. If there is any active phone with a last line number greater than this limit, warning information is displayed for phone reset.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ 7910—Cisco IP Phone 7910. ■ 7935—Cisco IP Phone 7935. ■ 7940—Cisco IP Phone 7940. ■ 7960—Cisco IP Phone 7960. ■ max-lines—Maximum number of DNs. The range is from 1 to 6. The default is 6.
max-dn <i>max-directory-numbers</i>	<p>To set the maximum number of DNs or virtual voice ports that can be supported by a router, use the max-dn command in call-manager-fallback configuration mode. To reset to the default, use the no form of this command.</p> <p>Note: You must reboot the router in order to reduce the limit of the DNs or virtual voice ports after the maximum allowable number is configured.</p> <p>Maximum number of directory numbers or virtual voice ports supported by the router. The maximum number is platform-dependent. The default is 0.</p> <p>Here are the number of DNs that are associated with each type of Cisco IP Phone:</p> <ul style="list-style-type: none"> ■ Cisco 1750—96 DNs ■ Cisco 1751—96 DNs ■ Cisco 2600 Series—96 DNs ■ Cisco 2600-XM Series—96 DNs ■ Cisco 2691—192 DNs ■ Cisco 3620—96 DNs ■ Cisco IAD2420 Series IADs—96 DNs

Command	Description
	<ul style="list-style-type: none"> ■ Cisco 3640—192 DNs ■ Cisco 3660—288 DNs ■ Cisco 3725—192 DNs ■ Cisco 3745—192 DNs ■ Cisco 3810-V3—96 DNs
max-ephones <i>max-phones</i>	<p>To configure the maximum number of Cisco IP Phones that can be supported by a router, use the max-ephones command in call-manager-fallback configuration mode. To reset to the default, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>max-phones</i>—Maximum number of phones that are supported by the router. The maximum number is version- and platform-dependent. For a range of values, refer to Cisco IOS CLI help. The default is 0.
network <i>ip-address</i> [<i>mask</i> <i>prefix-length</i>]	<p>To configure the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server, use the network command in DHCP pool configuration mode. To remove the subnet number and mask, use the no form of this command.</p> <p>This command has these arguments:</p> <ul style="list-style-type: none"> ■ <i>network-number</i>—The IP address of the DHCP address pool. ■ <i>mask</i>—(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host. ■ <i>prefix-length</i>—(Optional) The number of bits that constitute the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
show ccm-manager [backhaul config-download fallback-mgcp hosts music-on-hold redundancy]	<p>To display a list of Cisco CallManager servers and their current status and availability, use the show ccm-manager command in privileged EXEC mode.</p> <p>Note: For this lab the show ccm-manager fallback-mgcp command will be used.</p> <p>The command has these keywords:</p> <ul style="list-style-type: none"> ■ backhaul—(Optional) Displays PRI backhaul link information only. ■ config-download—(Optional) Displays information about the status of the MGCP configuration download. ■ fallback-mgcp—(Optional) Displays the status of the MGCP gateway fallback feature. ■ hosts—(Optional) Displays a list of each configured Cisco CallManager server in the network, together with its operational status and host IP address. ■ music-on-hold—(Optional) Displays information about all the multicast MOH sessions in the gateway at any given point in time.

Command	Description
	<ul style="list-style-type: none"> ■ redundancy—(Optional) Displays failover mode and status information for hosts, including the redundant link port, failover interval, keepalive interval, MGCP traffic time, switchover time, and switchback mode.
<pre>system message {primary primary-string secondary secondary-string}</pre>	<p>Declares the text for the system display message on Cisco IP Phones in fallback mode.</p> <p>This command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ primary <i>primary-string</i>—For Cisco IP Phones that can support static text messages during fallback, such as the Cisco IP Phone 7905, 7940 and 7960 units. A string of approximately 27 to 30 characters is allowed. ■ secondary <i>secondary-string</i>—For Cisco IP Phones that do not support static text messages, such as the Cisco IP Phone 7910. A string of approximately 20 characters is allowed.
<pre>time-format {12 24}</pre>	<p>Sets the time display format on all Cisco IP Phones that are registered with the router. The default is set to a 12-hour clock.</p>
<pre>user-locale country-code</pre>	<p>Selects a language for display on the Cisco IP Phone 7940G and Cisco IP Phone 7960G.</p> <p>If you have Cisco CallManager v3.2 or later, enter one of these ISO-3166 country codes:</p> <ul style="list-style-type: none"> ■ Denmark—DK ■ France—FR ■ Germany—DE ■ Italy—IT ■ The Netherlands—NL ■ Norway—NO ■ Portugal—PT ■ Russian Federation—RU ■ Spain—ES ■ Sweden—SE ■ United States—US (default)

Job Aids

There are no job aids for this lab activity.

Task 1: Configure SRST to Support Cisco IP Phones

Armstrong Snow Shovel is concerned that deploying a centralized call-processing model may initially expose the company to unplanned telephony outages if the Cisco IP Phones at BR1 lose connectivity to the Cisco CallManager cluster or if the IP WAN fails. Configure the gateway at BR1 so that the IP Phones will continue to function in the event of a loss of connectivity to the Cisco CallManager cluster or if the IP WAN fails.

Activity Procedure

Complete these steps:

- Step 1** Configure the BR1 gateway to support SRST. There should be a maximum of 12 DN's and 6 phones.
- Step 2** Configure the gateway so that when SRST is operational, the IP Phones maintain communication with the gateway every 20 seconds.
- Step 3** Configure the dial plan in the gateway to support SRST operation as a fallback from MGCP. There should be no loss of dialing capability when SRST is operational.
- Step 4** Configure the dial plan in the gateway to support inbound calls. The PSTN sends 10 digits for long-distance calls to BR1 but sends only 7 digits for local calls to BR1. Your dial plan should be configured so that calls from HQ are routed to the correct phone. In addition, extension 3001 should be able to call extension 3005 by dialing "93xx3005".
- Step 5** Configure SRST to support these phone functions:
 - The locale should be the United States.
 - The date is displayed on the phone.
 - A message tells the user that SRST v3.2 has been enabled.
- Step 6** Ensure that when SRST is active, calls to HQ are routed properly. Configure the appropriate dial peers so that users at BR1 can reach users at HQ.

Activity Verification

You have completed this task when you attain these results:

- You can verify that SRST is enabled if the IP WAN fails or if communication is lost to the Cisco CallManager.
- You can verify that calls are properly routed when SRST is enabled.

Lab 4-1 Answer Key: Configuring SRST

When you complete this activity, your configuration will be similar to the results here, with differences that are specific to your device or workgroup. This solution was developed on pod 8. The solution should be adjusted to match the dial plan for your assigned pod.

Task 1 Solution

Step 1 Configure SRST service. Type these commands in BR1:

```
call-manager-fallback
max-ephones 6
max-dn 12
ip source-address 10.2.120.1
dialplan-pattern 1 3083083... extension-length 4
```

Step 2 Configure keepalive timers. Type this command in BR1:

```
keepalive 20
```

Step 3 Configure MGCP fallback and appropriate dial peers to support PSTN calls. Type these commands on BR1:

```
ccm-manager fallback-mgcp
call application alternate default
dial-peer voice 1 pots
incoming called-number .
direct-inward-dial
port 1/0:23
!
dial-peer voice 911 pots
destination-pattern 911
prefix 911
port 1/0:23
!
dial-peer voice 9911 pots
destination-pattern 9911
prefix 911
port 1/0:23
!
dial-peer voice 97 pots
destination-pattern 9[2-9].....
forward-digits 7
port 1/0:23
!
dial-peer voice 910 pots
destination-pattern 91[2-9]..[2-9].....
forward-digits 11
port 1/0:23
!
dial-peer voice 9011 pots
destination-pattern 9011T
prefix 011
port 1/0:23
```

Step 4 The **dialplan-pattern** command can be configured to support only one E.164 number per extension range. Because the PSTN is sending both 7- and 10-digit DNIS for calls at BR1, a different method must be used to routes calls to the appropriate phone. You can employ several digit manipulation techniques to accomplish this task. The solution that follows uses a voice translation rule to truncate incoming called numbers to the last four digits.

Step 5 Type these commands on BR1:

```
voice translation-rule 1
 rule 1 /^.*\(...)\ / /\1/
 voice translation-profile 4digit
 translate called 1
 dial-peer voice 1 pots
 translation-profile incoming 4digit
```

Step 6 Configure locale and phone display. Type these commands on BR1:

```
call-manager-fallback
 user-locale US
 system message primary SRST 3.2 has been enabled
```

Step 7 Configure dial peers to support four-digit dialing to HQ and BR2. Type these commands on BR1:

```
dial-peer voice 2000 pots
 destination-pattern 2...
 prefix 12082082
 port 1/0:23

dial-peer voice 4000 pots
 destination-pattern 4...
 prefix 011440888084
 port 1/0:23
```

Lab 4-2: Configuring DSP Farms

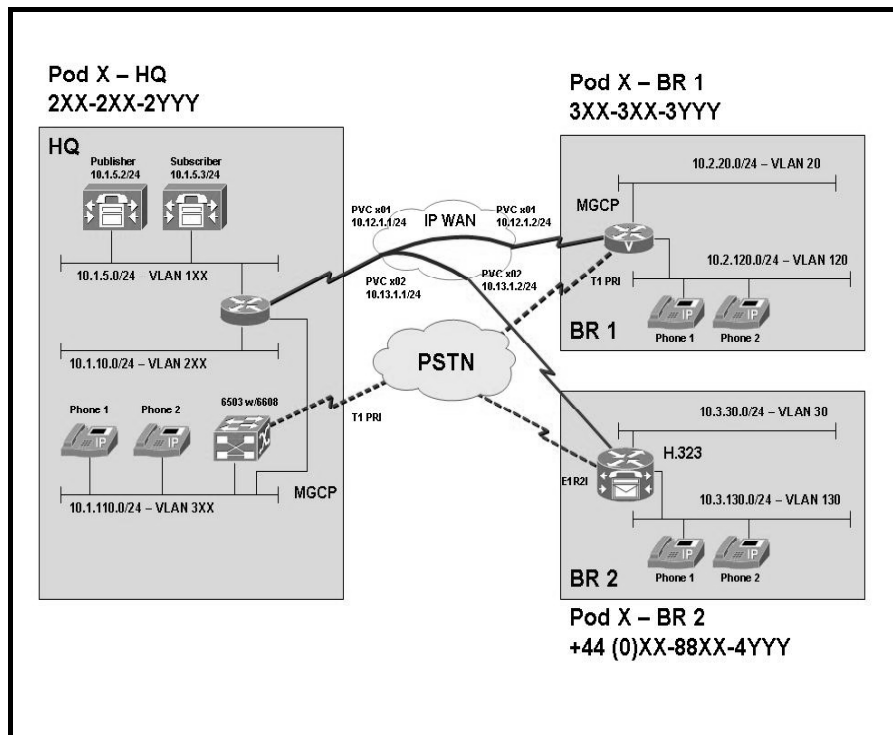
Complete this lab activity to practice what you learned in the related module.

Activity Objective

In this activity, you will configure a DSP farm at the BR1 location to support transcoding and conferencing

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Student Pods

The student pod equipment requirements are as follows:

- Six Cisco IP Phones, which can be any model except for 7920. The IP Phones require power from either an in-line power switch or external power bricks.
- One Cisco router with one 10/100 Ethernet interface, one T1 serial interface, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one T1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one E1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco Catalyst 3550 switch for each branch location or one internal EtherSwitch module for the router.
- One Cisco Catalyst 6500 switch with one 10/100 Ethernet switch module and one WS-X6608 gateway module for the HQ location.
- One Cisco CallManager publisher and subscriber.

Network Core

The network core equipment requirements are as follows:

- One Cisco router to provide Frame Relay or ATM support to an IP WAN to connect the HQ with BR1 and BR2.
- One Cisco CallManager and one Cisco router configured as an MGCP gateway to provide the functionality of the PSTN to all locations.

Command List

The table describes the commands that are used in this activity.

DSP Farm Configuration Commands

Command	Description
<code>associate application sccp</code>	To associate SCCP to the DSP farm profile, use the associate application command in DSP farm profile configuration mode. To remove the protocol, use the no form of this command. This command has no keywords or arguments.

Command	Description
<code>codec codec-type</code>	<p>To specify the codecs that are supported by a DSP farm profile, use the codec command in DSP farm profile configuration mode. To remove the codec, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>codec-type</i>—Specifies the codec that is preferred. The codec options are as follows: ■ g711alaw—G.711 a-law 64,000 bps. ■ g711ulaw—G.711 u-law 64,000 bps. ■ g729abr8—G.729 Annex A and B 8000 bps. ■ g729br8—G.729 Annex B 8000 bps. ■ g729ar8—G.729 Annex A and R 8000 bps. ■ g729r8—G.729 8000 bps. ■ gsmefr—GSMEFR 12,200 bps. ■ gsmfr—GSMFR 13,200 bps.
<code>configure terminal</code>	Enters global configuration mode.
<code>connect interval seconds</code>	<p>(Optional) To specify the amount of time that a given DSP farm profile waits before attempting to connect to a Cisco CallManager when the current Cisco CallManager fails to connect, use the connect interval command in SCCP Cisco CallManager configuration mode. To reset to the default value, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>seconds</i>—Timer value, in seconds. The range is from 1 to 3600. The default is 60.
<code>connect retries number</code>	<p>(Optional) To specify the number of times that a DSP farm attempts to connect to a Cisco CallManager when the current Cisco CallManager connections fails, use the connect retries command in SCCP Cisco CallManager configuration mode. To reset this number to the default value, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>number</i>—Number of connection attempts. The range is from 1 to 32. The default is 3.
<code>debug dspfarm {all errors events packets}</code>	<p>To display DSP farm service debugging information, use the debug dspfarm command in privileged EXEC mode. To disable debugging output, use the no form of this command.</p> <p>The command has these keywords:</p> <ul style="list-style-type: none"> ■ all—All DSP farm debug trace information. ■ errors—DSP farm errors. ■ events—DSP farm events. ■ packets—DSP farm packets.

Command	Description
<code>debug media resource provisioning {all errors events}</code>	<p>The command has these keywords:</p> <ul style="list-style-type: none"> ■ all—To display debugging messages that are related to all media resource provisioning. ■ errors—To display debugging messages that are related to media resource provisioning errors. ■ events—To display debugging messages that are related to media resource provisioning events.
<code>debug sccp {all errors events packets parser}</code>	<p>The command has these keywords:</p> <ul style="list-style-type: none"> ■ all—All SCCP debug trace information. ■ errors—SCCP errors. ■ events—SCCP events. ■ packets—SCCP packets. ■ parser—SCCP parser and builder.
<code>description text</code>	<p>To include a description about the DSP farm profile, use the description command in DSP farm profile configuration mode. To remove a description, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ text—Character string from 1 to 80 characters.
<code>dspfarm profile profile-identifier {conference mtp transcode}</code>	<p>To enter DSP farm profile configuration mode and define a profile for DSP farm services, use the dspfarm profile command in global configuration mode. To delete a disabled profile, use the no form of this command.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ profile-identifier—Number that uniquely identifies a profile. The range is from 1 to 65535. There is no default. ■ conference—Enables profile for conferencing. ■ mtp—Enables profile for MTP. ■ transcode—Enables profile for transcoding.
<code>dsp services dspfarm</code>	<p>To configure DSP farm services for a particular digital T1 or E1 packet voice trunk network module (NM-HDV) or HDV transcoding or conferencing DSP farm (NM-HDV-FARM), use the dsp services dspfarm command in interface configuration mode. To disable services, use the no form of this command.</p> <p>This command has no arguments or keywords.</p>
<code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
<code>end</code>	Exits to privileged EXEC mode.
<code>exit</code>	Exits global configuration mode.
<code>gateway</code>	Enters gateway configuration mode.

Command	Description
<code>keepalive timeout seconds</code>	<p>(Optional) To set the length of time between keepalive messages from SCCP to Cisco CallManager, use the keepalive timeout command in SCCP Cisco CallManager configuration mode. To reset the length of time to the default value, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ seconds—Time between keepalive messages. The range is from 1 to 180. The default is 30.
<code>maximum sessions number</code>	<p>To specify the maximum number of sessions that are supported by the profile, use the maximum sessions command in DSP farm profile configuration mode. To reset to the default, use the no form of the command.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ hardware—Number of sessions that MTP hardware resources will support. ■ software—Number of sessions that MTP software resources will support. ■ number—Number of sessions that are supported by the profile. The range is 0 to x. The default is 0. The x value is determined at run time depending on the number of resources that are available with the resource provider.
<code>no shutdown</code>	<p>Enables the profile, allocates DSP farm resources, and associates the application.</p>
<code>registration retries retry-attempts</code>	<p>(Optional) To set the number of times that SCCP tries to register with a Cisco CallManager, use the registration retries command in SCCP Cisco CallManager configuration mode. To reset this number to the default value, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ retry-attempts—Number of registration attempts. The range is from 1 to 32. The default is 3.
<code>registration timeout timeout-value</code>	<p>(Optional) To set the length of time between registration messages sent from SCCP to Cisco CallManager, use the registration timeout command in SCCP Cisco CallManager configuration mode. To reset the length of time to the default value, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ timeout-value—Time, in seconds, between registration messages. The range is from 1 to 180. The default is 3.
<code>sccp</code>	<p>To enable SCCP and its related applications (transcoding and conferencing), use the sccp command in global configuration mode. To disable the protocol, use the no form of this command.</p> <p>This command has no arguments or keywords.</p>

Command	Description
<p>For NM-HDV2, NM-HD-1V, NM-HD-2V, or NM-HD-2VE using Cisco IOS Release 12.3(8)T or later:</p> <pre>sccp ccm {ip-address dns} identifier identifier-number [port port-number] [version version-number]</pre> <p>For NM-HDV using Cisco IOS Release 12.2(13)T or later, and Cisco 1751 or Cisco 1760 using IOS Release 12.3(8)T or later:</p> <pre>sccp ccm {ip-address dns} priority priority [port port-number] [version version-number]</pre>	<p>To add a Cisco CallManager server to the list of available servers and to set various parameters—including address or DNS name, priority (if more than one server is available), port number, and version number—use the sccp ccm command in global configuration mode. To remove a particular server from the list, use the no form of this command.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ <i>ip-address</i>—IP address of the Cisco CallManager server. ■ <i>dns</i>—DNS name. ■ priority <i>priority</i>—Priority of this Cisco CallManager server relative to other connected servers. The range is from 1 (highest) to 4 (lowest). ■ port <i>port-number</i>—(Optional) TCP port number. ■ version 3.0 3.1+—Cisco CallManager version: version 3.0 or version 3.1 and higher.
<pre>sccp ccm group group- number</pre>	<p>To create a Cisco CallManager group and enter SCCP Cisco CallManager configuration mode, use the sccp ccm group command in global configuration mode. To remove a particular Cisco CallManager group, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>group-number</i>—Number that identifies the Cisco CallManager group. The range is from 1 to 65535. There is no default value.
<pre>sccp ip precedence value</pre>	<p>To set the IP precedence value to be used by SCCP, use the sccp ip precedence command in global configuration mode. To reset to the default, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>value</i>—IP precedence value. The range is from 1 (highest) to 7 (lowest).
<pre>sccp local interface-type interface-number</pre>	<p>To select the local interface that the SCCP applications (transcoding and conferencing) should use to register with Cisco CallManager, use the sccp local command in global configuration mode. To deselect the interface, use the no form of this command.</p> <p>The command has these arguments:</p> <ul style="list-style-type: none"> ■ <i>interface-type</i>—Interface type that the SCCP application uses to register with Cisco CallManager. The type can be an interface address or a virtual-interface address such as Ethernet. ■ <i>interface-number</i>—Interface number that the SCCP application uses to register with Cisco CallManager.

Command	Description
<pre>show dspfarm [all dsp {active all idle} sessions]</pre>	<p>The command has these keywords:</p> <ul style="list-style-type: none"> ■ all—(Optional) All DSP farm global information. ■ dsp—(Optional) DSP farm DSP information. ■ active—(Optional) Information about active DSPs. ■ all—(Optional) Information about all DSP farm DSPs. ■ idle—(Optional) Information about the idle DSPs. ■ sessions—(Optional) Information about DSP farm sessions and connections.
<pre>show dspfarm profile [profile-identifier]</pre>	<p>To display configured digital signal processor (DSP) farm profile information for a selected Cisco CallManager group, use the show dspfarm profile command in privileged EXEC mode.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>profile-identifier</i>—(Optional) Number that uniquely identifies a profile. The range is from 1 to 65535. There is no default.
<pre>show media resource status</pre>	<p>To display the current media resource status, use the show media resource status command in privileged EXEC mode.</p> <p>This command has no arguments or keywords.</p>
<pre>show sccp ccm group [group-number]</pre>	<p>To display the groups that are configured on a specific Cisco CallManager, use the show sccp ccm group command in privileged EXEC mode.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>group-number</i>—(Optional) Number that identifies the Cisco CallManager group. The range is from 1 to 65535. There is no default value.
<pre>show sccp connections details</pre>	<p>To display the SCCP connections details such as call leg details, use the show sccp connections details command in privileged EXEC mode.</p> <p>This command has no arguments or keywords.</p>
<pre>show voice dsp</pre>	<p>To show the current status of all DSP voice channels, use the show voice dsp command in privileged EXEC mode.</p> <p>The command has these keywords:</p> <ul style="list-style-type: none"> ■ active—Show DSP active channels. ■ crash-dump—Show DSP crash dump facility. ■ detailed—Show detailed DSP status. ■ group—Show DSP group information. ■ signaling—Show DSP signaling channel usage. ■ voice—Show DSP voice channel usage. ■ —Output modifiers.

Command	Description
switchback interval <i>seconds</i>	<p>(Optional) To set the amount of time that the DSP farm waits before polling the primary Cisco CallManager when the current Cisco CallManager switchback connection fails, use the switchback interval command in SCCP Cisco CallManager configuration mode. To reset the amount of time to the default value, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ seconds—Timer value, in seconds. The range is from 1 to 3600. The default is 60.
switchback method { graceful guard [<i>guard-timeout-value</i>] immediate uptime <i>uptime-timeout-value</i> }	<p>(Optional) To set the Cisco CallManager switchback method, use the switchback method command in Skinny SCCP Cisco CallManager configuration mode. To reset to the default value, use the no form of this command.</p> <p>Default is guard, with a timeout value of 7200 seconds.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ graceful—Selects the graceful switchback method. ■ guard—Selects the graceful-with-guard switchback method. ■ <i>guard-timeout-value</i>—(Optional) Timeout value, in seconds. The range is from 60 to 172800. The default is 7200. ■ immediate—Selects the immediate switchback method. ■ uptime—Selects the uptime-delay switchback method. ■ <i>uptime-timeout-value</i>—(Optional) Timeout value, in seconds. The range is from 60 to 172800. The default is 7200.
switchover method { graceful immediate }	<p>(Optional) To set the switchover method that the SCCP client uses when the communication link between the active Cisco CallManager and the SCCP client goes down, use the switchover method command in SCCP Cisco CallManager configuration mode. To reset the switchover method to the default, use the no form of this command.</p> <p>The command has these keywords:</p> <ul style="list-style-type: none"> ■ graceful—Switchover happens only after all the active sessions are terminated gracefully. ■ immediate—Switches over to any one of the secondary Cisco CallManager systems immediately.
timer receive-rtp <i>seconds</i>	<p>To configure the RTP timeout interval to clear hanging connections, use the timer receive-rtp command in gateway configuration mode. To reset the timer to the default value, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ seconds—Timer value, in seconds. The range is from 180 to 1800. The default is 1200.
voice-card <i>slot</i>	<p>To enter voice card configuration mode and configure a voice card, use the voice-card command in global configuration mode.</p>

Command	Description
	<p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>slot</i>—Slot number for the card to be configured. These platform-specific numbering schemes apply: <ul style="list-style-type: none"> — • For the Cisco 2600 Series and Cisco 2600XM: <ul style="list-style-type: none"> ■ – 0 is the AIM slot. ■ – 1 is the network module slot. — • For the Cisco 3600 Series: <ul style="list-style-type: none"> ■ – 1 to 6 are the network module slots. — • For the Cisco 3660: <ul style="list-style-type: none"> ■ – 7 is AIM slot 0. ■ – 8 is AIM slot 1. — • For the Cisco MC3810 with one or two HCMs installed: <ul style="list-style-type: none"> ■ – 0 applies to the entire chassis.

Job Aids

There are no job aids for this lab activity.

Task 1: Configure DSP Farm

The IP telephony network at Armstrong Snow Shovel has a need to support conferencing and transcoding resources. These resources need to be deployed across the network, but initially the company would like to evaluate how they work at BR1. Configure the DSP farm to support one conferencing resource. The resources should support G.711 through G.729 transcoding.

Activity Procedure

Complete these steps:

- Step 1** Evaluate the DSP resources in the BR1 gateway to determine if there are enough DSP resources to support Armstrong Snow Shovel requirements.
- Step 2** Configure the DSP farm on the BR1 gateway. Pay particular attention to the network module that is being configured.
- Step 3** Configure the local interface so that the DSP farm can register with the Cisco CallManager cluster at HQ.
- Step 4** Configure conference bridge support on the Cisco CallManager cluster.

Activity Verification

You have completed this task when you attain these results:

You can use the appropriate **show** and **debug** commands to verify that the DSP farm has registered with the Cisco CallManager cluster at HQ.

Lab 4-2 Answer Key: Configuring DSP Farms

When you complete this activity, your configuration will be similar to the results here, with differences that are specific to your device or workgroup:

Task 1 Solution

Step 1 Use the **show voice dsp detailed** command to examine the number and type of DSPs that are located on the voice card in your gateway. The output from this command will show DSP type, complexity, number, current state, and voice port.

Step 2 Step 2 requires you to enable the DSP farm. Type these commands on BR1:

```
voice-card 1
dspfarm
dsp services dspfarm
```

Step 3 Step 3 configures the gateway to register with the Cisco CallManager systems and sets the maximum number of conferencing sessions. Type these commands on BR1:

```
sccp local Vlan120 (This could be a physical interface.)
sccp ccm 10.1.5.3 priority 1
sccp ccm 10.1.5.2 priority 2
sccp
dspfarm confbridge maximum sessions 1
dspfarm
```

The Cisco IOS conference bridge will need to register with the Cisco CallManager before it can begin supporting conferences. The conferencing service needs to be configured as an IOS gateway. The name of the conference bridge is CFB The dots represent the MAC address of the interface that you have identified in the previous step. You will need to make sure that the conference bridge is associated with the correct device pool. Because this conference bridge is going to be at the BR1 location, the BR1 device pool should be selected. After the configuration is complete, save and reset the conference bridge.

Step 4 Now go back to the BR1 gateway and use the **show dsp all** command. You should now see that the conference bridge is active.

Lab 4-3: Configuring TCL Scripts

Complete this lab activity to practice what you learned in the related module.

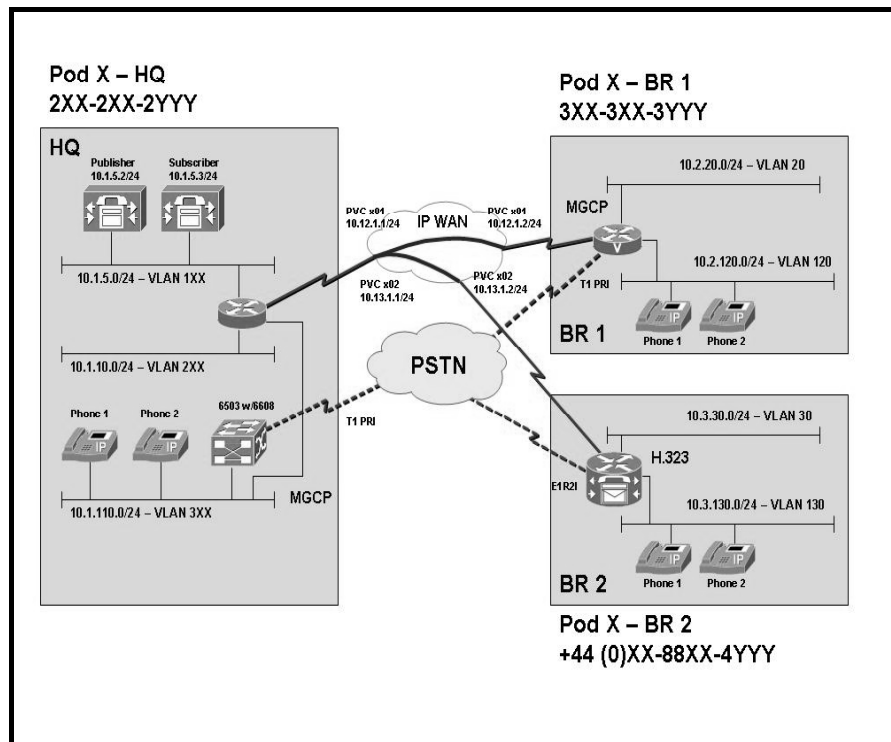
Activity Objective

In this activity, you will deploy TCL scripts to function as an Auto Attendant at site 2. The TCL script/Auto Attendant function will be operational only when SRST is operational. After completing this activity, you will be able to meet these objectives:

- Configure TCL on a Cisco IOS gateway
- Enable TCL scripts to operate with SRST only when SRST is operational
- Verify TCL script operation

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Student Pods

The student pod equipment requirements are as follows:

- Six Cisco IP phones, which can be any model except for 7920. The IP Phones require power from either an in-line power switch or external power bricks.
- One Cisco router with one 10/100 Ethernet interface, one T1 serial interface, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one T1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one E1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco Catalyst 3550 switch for each branch location or an internal EtherSwitch module for the router.
- One Cisco Catalyst 6500 with one 10/100 Ethernet switch module and one WS-X6608 gateway module for the HQ location.
- One Cisco CallManager publisher and subscriber.

Network Core

The network core equipment requirements are as follows:

- One Cisco router to provide Frame Relay or ATM support to an IP WAN to connect the HQ with BR1 and BR2.
- One Cisco CallManager and one Cisco router configured as an MGCP gateway to provide the functionality of the PSTN to all locations.

Command List

The table describes the commands that are used in this activity.

TCL Script Configuration Commands

Command	Description
<code>call application voice application-name location [word]</code>	<p>To define the name of a voice application and specify the location of the TCL or VXML document to load for this application, use the call application voice command in global configuration mode. To remove the defined application and all configured parameters that are associated with it, use the no form of this command.</p> <p>The command has these arguments:</p> <ul style="list-style-type: none">■ <i>application-name</i>—Character string that defines the name of the voice application.

	<ul style="list-style-type: none"> ■ <i>location</i>—Location of the TCL file or VXML document in URL format. Valid storage locations are TFTP, FTP, HTTP, and Flash memory. ■ <i>word</i>—(Optional) Text string that defines an attribute-value pair that is specified by the TCL script and understood by the RADIUS server.
<p>configure terminal</p>	<p>Enters global configuration mode.</p>
<p>For Cisco 1750 and Cisco 1751 Modular Access Routers and Cisco 2600 Series:</p> <pre>dial-peer voice tag {pots vofr voip} no dial-peer voice tag {pots vofr voip}</pre> <p>For Cisco 2600 Series, 2600XM, 3600 Series, 3700 Series, IAD2420 Series, and VG200:</p> <pre>dial-peer voice tag {pots voatm vofr voip} no dial-peer voice tag {pots voatm vofr voip}</pre> <p>For Cisco 7200 Series:</p> <pre>dial-peer voice tag {vofr} no dial-peer voice tag {vofr}</pre> <p>For Cisco 7204VXR and Cisco 7206VXR:</p> <pre>dial-peer voice tag {pots voatm vofr voip} no dial-peer voice tag {pots voatm vofr voip}</pre> <p>For Cisco AS5300:</p> <pre>dial-peer voice tag {mmoip pots vofr voip} no dial-peer voice tag {mmoip pots vofr voip}</pre> <p>For Cisco MC3810:</p> <pre>dial-peer voice tag {pots voatm vofr} no dial-peer voice tag {pots voatm vofr}</pre>	<p>To define a particular dial peer, to specify the method of voice encapsulation, and to enter dial-peer configuration mode, use the dial-peer voice command in global configuration mode. To delete a defined dial peer, use the no form of this command. Alternately, to disable a dial peer, use the no shutdown command in dial-peer configuration mode.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ <i>tag</i>—Digits that define a particular dial peer. The range is from 1 to 2147483647. ■ mmoip—Indicates that this is a multimedia mail peer that uses IP encapsulation on the IP backbone. ■ pots—Indicates that this is a POTS peer that uses VoIP encapsulation on the IP backbone. ■ voatm—Specifies that this is a VoATM dial peer that uses real-time AAL5 voice encapsulation on the ATM backbone network. ■ vofr—Specifies that this is a VoFR dial peer that uses FRF.11 encapsulation on the Frame Relay backbone network. ■ voip—Indicates that this is a VoIP peer that uses voice encapsulation on the POTS network.

<pre>debug isdn q931</pre>	<p>To display information about call setup and teardown of ISDN network connections (Layer 3) between the local router (user side) and the network, use the debug isdn q931 command in privileged EXEC mode. To disable debugging output, use the no form of this command.</p>
<pre>show call application voice [name summary]</pre>	<p>To display information about voice applications, use the show call application voice command in EXEC mode.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ name—(Optional) Name of the desired voice application. Output displays information about that application. ■ summary—(Optional) Output displays a one-line summary of each voice application.
<pre>show dial-peer voice [number summary]</pre>	<p>To display information for voice dial peers, use the show dial-peer voice command in EXEC mode.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ number—(Optional) A specific voice dial peer. Output displays detailed information about that dial peer. ■ summary—(Optional) Output displays a short summary of each voice dial peer.
<pre>show running-config [options]</pre>	<p>To display the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class, use the show running-config command in privileged EXEC mode.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ options—(Optional) You can enter one of these options with the command: <ul style="list-style-type: none"> — brief—Displays the configuration without certification data. — class-map name—Displays class map information. The linenum keyword can be used with the class-map name option. — full—Displays the full configuration. — interface type number—Displays interface-specific configuration information. If you use the interface keyword, you must specify the interface type and the interface number (for example, interface ethernet 0). Common interfaces include async, ethernet, fastEthernet, group-async, loopback, null, serial, and virtual-template. Use the show run interface ? command to determine the interfaces available on your system. — linenum—Displays line numbers in the output. The brief or full keyword can be used with the linenum keyword. — map-class—Displays map class information. This option is described separately; see the show running-config map-class command page.

	<ul style="list-style-type: none">— policy-map name—Displays policy map information. The linenum keyword can be used with the policy-map name option.— vc-class name—Displays VC class information (display available only on limited routers such as the Cisco 7500 Series). The linenum keyword can be used with the vc-class name option.— —Allows addition of output modifiers and is available with all the keywords for this command.
--	---

Job Aids

There are no job aids for this lab activity.

Task 1: Configure TCL Scripts on Site 1 Gateway

The staff at BR1 is relatively small and does not have a dedicated receptionist. During normal operation the receptionist at HQ manages calls for the staff at BR1. Armstrong Snow Shovel would like to have a similar capability in the event of an IP WAN failure or loss of communication to the Cisco CallManager cluster. The BR1 gateway needs to be configured to support a TCL script that will provide Auto Attendant functions when SRST is operational.

Activity Procedure

Configure the BR1 gateway to use the preloaded Auto Attendant TCL script. The TCL script software is located in Flash memory on each BR1 router. You should use this script only when SRST is operational. The telephone pilot number that callers use to reach the BR1 Auto Attendant is 30X-30X-3000.

Activity Verification

You have completed this task when you attain these results:

- Verify that direct dialed numbers still go to the appropriate extensions without Auto Attendant intervention.
- When SRST is operational, verify that the Auto Attendant answers the call and you can dial digits so that an extension will ring. .
- Test the SRST operation to ensure that TCL is providing Auto Attendant functionality. Then restore connectivity to BR1 and test again to ensure that SRST is no longer functioning and TCL is no longer active.

Lab 4-3 Answer Key: Configuring TCL Scripts

When you complete this activity, your configuration will look similar to the results here, with differences that are specific to your device or workgroup:

Task 1 Solution

Step 1 To configure the Auto Attendant TCL script, first go and examine the contents of Flash memory. You should see these files:

```
srst_CISCO.2.0.0.0.tcl
en_dest_busy.au
en_dest_unreachable.au
en_disconnect.au
en_enter_dest.au
en_reenter_dest.au
en_welcome.au
music-on-hold.au
```

Step 2 Next, configure the Auto Attendant in the gateway. Type these commands at the PodX-BR1(config)# prompt:

```
call application voice AA flash://srst_CISCO.2.0.0.0.tcl
```

In this command the name of the application is Auto Attendant and the path to the TCL script follows. In this lab you are serving the files from Flash, but you can also make this procedure work with an external TFTP server. Make sure that you are consistent in the use of the name that you have chosen for the script. Capitalization is critical.

Step 3 Next, configure the pilot that will be used when SRST is active:

```
call application voice AA aa-pilot 3000
```

This command sets the pilot number that the Auto Attendant will use when SRST is operating. You could change this to another number, but 3000 represents a logical choice.

Step 4 Set the language that will be used in the audio prompts:

```
call application voice AA language 1 en
```

This command sets the language that the TCL script will use. In this case the language is English. The digit that represents the language is critical. In testing, this value needs to be different than the value that is set in the next command.

Step 5 Set the location that the gateway will use for retrieving the audio files:

```
call application voice AA set-location en 0 flash://
```

This command sets the location for the audio files that the TCL script will use. This command can also support an external TFTP server.

Step 6 The last step is to apply the application to the incoming dial peer. In the router **dial-peer voice 1 pots** is configured. Type this command to configure the dial peer to support this application for incoming calls:

application AA

The application will be trigger when SRST is engaged, and the TCL script will become operational.

Lab 5-1: Configuring Gatekeepers

Complete this lab activity to practice what you learned in the related module.

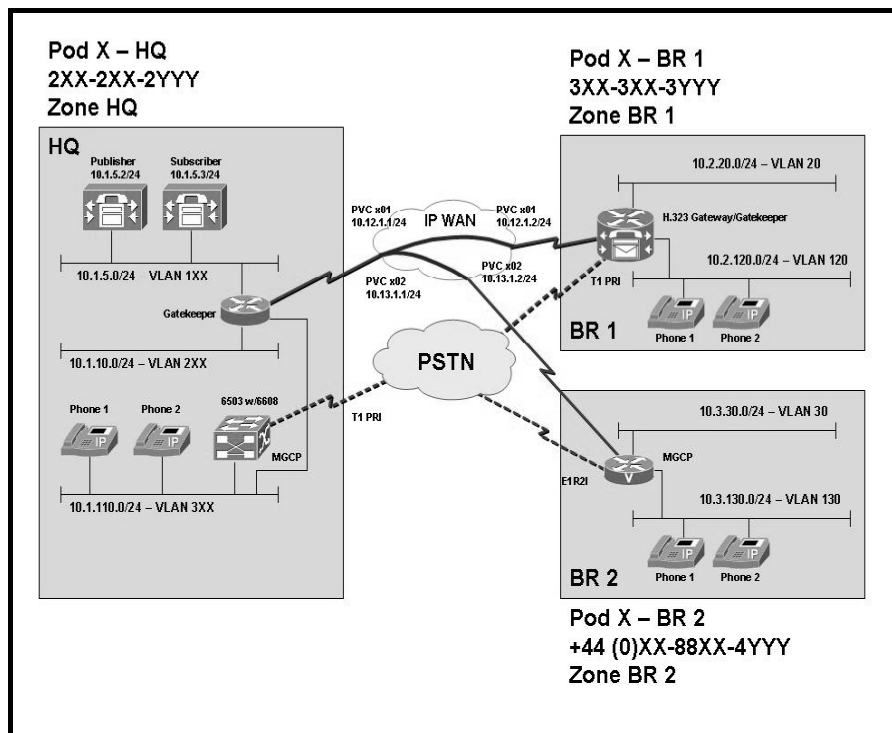
Activity Objective

In this activity, you will configure a gatekeeper to provide E.164 dial-plan resolution and CAC between HQ and BR2. After completing this activity, you will be able to meet these objectives:

- Configure an H.323 gatekeeper at HQ and BR2 to support interzone CAC and dial-plan resolution
- Test the dial-plan resolution and CAC by placing calls from HQ to BR2

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Student Pods

The student pod equipment requirements are as follows:

- Six Cisco IP phones, which can be any model except for 7920. The IP Phones require power from either an in-line power switch or external power bricks.
- One Cisco router with one 10/100 Ethernet interface, one T1 serial interface, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one T1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one E1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco Catalyst 3550 switch for each branch location or one internal EtherSwitch module for the router.
- One Cisco Catalyst 6500 switch with one 10/100 Ethernet switch module and one WS-X6608 gateway module for the HQ location.
- One Cisco CallManager publisher and subscriber.

Network Core

The network core equipment requirements are as follows:

- One Cisco router to provide Frame Relay or ATM support to an IP WAN to connect the HQ with BR1 and BR2.
- One Cisco CallManager and one Cisco router configured as an MGCP gateway to provide the functionality of the PSTN to all locations.

Command List

The table describes the commands that are used in this activity.

Gatekeeper Commands

Command	Description
<pre>bandwidth {interzone total session} {default zone zone-name} bandwidth-size</pre>	<p>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.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ 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 that is allowed in the zone. ■ session—Maximum bandwidth that is 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 10000000. For session, the range is from 1 to 5000.
<pre>debug gatekeeper gup {events asn1}</pre>	<p>To display the GUP events or ASN.1 details, use the debug gatekeeper gup command in privileged EXEC mode. To disable debugging output, use the no form of this command.</p> <p>The command has these keywords:</p> <ul style="list-style-type: none"> ■ events—Displays a message whenever a GUP announcement is sent or received. GUP is the protocol that is used between individual gatekeepers in a cluster; GUP keeps all the gatekeepers synchronized with all endpoints that are registered on the cluster. ■ asn1—ASN.1 library. ASN.1 is an ITU standard for protocol syntax and message encoding. Entering this keyword causes a packet dump of all GUP announcement messages.
<pre>debug gatekeeper load {events}</pre>	<p>To display gatekeeper load-balancing debug events, use the debug gatekeeper load command in privileged EXEC mode. To disable debugging output, use the no form of this command.</p> <p>The command has this keyword:</p> <ul style="list-style-type: none"> ■ events—Displays a message whenever a load-balancing message is sent or received.

Command	Description
<code>debug gatekeeper server</code>	To trace all the message exchanges between the Cisco IOS gatekeeper and the external applications, use the debug gatekeeper server command in privileged EXEC mode. To disable debugging output, use the no form of this command. This command has no arguments or keywords.
<code>gatekeeper</code>	Enters gatekeeper configuration mode.
<code>gw-type-prefix type-prefix</code> [[<i>hopoff gkid1</i>] [<i>hopoff gkid2</i>] [<i>hopoff gkidn</i>] [<i>seq</i> <i>blast</i>]] [<i>default-technology</i>] [[<i>gw ipaddr ipaddr</i> [<i>port</i>]]]	To configure a technology prefix in the gatekeeper, use the gw-type-prefix command in gatekeeper configuration mode. To remove the technology prefix, use the no form of this command. The command has these keywords and arguments: <ul style="list-style-type: none"> ■ <i>type-prefix</i>—The technology prefix is recognized and is stripped before you check for the zone prefix. It is strongly recommended that you select technology prefixes that do not lead to ambiguity with zone prefixes. Do this by using the # character to terminate technology prefixes, for example, 3#. ■ <i>hopoff gkid</i>—(Optional) Use this option to specify the gatekeeper where the call is to hop off, regardless of the zone prefix in the destination address. The <i>gkid</i> argument refers to a gatekeeper that was previously configured using the zone local or zone remote command. You can enter this keyword and argument multiple times to configure redundant gatekeepers for a given technology prefix. ■ <i>seq</i> <i>blast</i>—(Optional) If you list multiple hopoffs, these keywords indicate that the LRQs should be sent sequentially or simultaneously (blast) to the gatekeepers according to the order in which the gatekeepers were listed. The default is to send them sequentially. ■ <i>default-technology</i>—(Optional) Gateways that register with this prefix option are used as the default for routing any addresses that are otherwise unresolved. ■ <i>gw ipaddr ipaddr</i> [<i>port</i>]—(Optional) Use this option to indicate that the gateway is incapable of registering technology prefixes. When it registers, it adds the gateway to the group for this type of prefix, just as if it had sent the technology prefix in its registration. This parameter can be repeated to associate more than one gateway with a technology prefix.
<code>no shutdown</code>	Activates the gatekeeper.
<code>show gatekeeper calls</code>	To display the status of each ongoing call of which a gatekeeper is aware, use the show gatekeeper calls command in privileged EXEC mode. This command has no arguments or keywords. show gatekeeper calls field descriptions are as follows <ul style="list-style-type: none"> ■ LocalCallID —Identification number of the call. ■ Age(secs)—Age of the call, in seconds. ■ BW(Kbps)—Bandwidth in use, in kilobytes per second.

Command	Description
	<ul style="list-style-type: none"> ■ Ends—Role of each endpoint (terminal, gateway, or proxy) in the call (originator, target, or proxy) and the call-signaling and RAS protocol address. ■ Alias—H.323 ID or e-mail ID of the endpoint. ■ E.164Addr—E.164 address of the endpoint. ■ CallSignalAddr—Call-signaling IP address of the endpoint. ■ Port—Call-signaling port number of the endpoint. ■ RASSignalAddr—RAS IP address of the endpoint. ■ Port—RAS port number of the endpoint.
<pre>show gatekeeper circuits [begin exclude include] <i>expression</i></pre>	<p>To display the circuit information on a gatekeeper, use the show gatekeeper circuits command in privileged EXEC mode.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ begin—(Optional) Displays all circuits, beginning with the line that contains the expression. ■ exclude—(Optional) Displays all circuits, excluding those that contain the expression. ■ include—(Optional) Displays all circuits, including those that contain the expression. ■ <i>expression</i>—(Optional) Word or phrase that is used to determine what lines are displayed. <p>show gatekeeper circuits field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ Circuit—Name of each circuit that is connected to the gatekeeper. ■ Endpoint—Name of each H.323 endpoint. ■ Max Calls—Maximum number of calls that the circuit can handle. ■ Avail Calls—Number of new calls that the circuit can handle at the current time. ■ Resources—Indicates whether circuit resources have exceeded the defined threshold limits. The endpoint resource-threshold command defines these thresholds. ■ Zone—Zone that supports the endpoint. The zone circuit-id command assigns a zone to an endpoint. ■ Total Endpoints—Total number of endpoints that are supported by the circuit. ■ Total Zones—Total number of zones that are supported by the circuit.
<pre>show gatekeeper endpoint circuits [begin exclude include] <i>expression</i></pre>	<p>To display the information of all registered endpoints and carriers or trunk groups for a gatekeeper, use the show gatekeeper endpoint circuits command in privileged EXEC mode.</p> <p>The command has these keywords and arguments:</p>

Command	Description
	<ul style="list-style-type: none"> ■ begin—(Optional) Displays all circuits, beginning with the line that contains <i>expression</i>. ■ exclude—(Optional) Displays all circuits, excluding those that contain <i>expression</i>. ■ include—(Optional) Displays all circuits, including those that contain <i>expression</i>. ■ <i>expression</i>—(Optional) Word or phrase that is used to determine what lines are displayed. <p>show gatekeeper endpoint circuits field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ CallSignalAddr—Call-signaling IP address of the endpoint. If the endpoint is also registered with an alias, a list of all aliases that are registered for that endpoint should be listed on the line below. ■ Port—Call-signaling port number of the endpoint. ■ RASSignalAddr—RAS IP address of the endpoint. ■ Port—RAS port number of the endpoint. ■ Zone Name—Zone name (gatekeeper ID) that this endpoint registered in. ■ Type—Endpoint type (for example, terminal, gateway, or MCU). ■ Flags - S—The endpoint is statically entered from the alias command rather than being dynamically registered through RAS messages. ■ O—The endpoint, which is a gateway, has sent notification that it is nearly out of resources. ■ E164-ID—E.164 ID of the endpoint. ■ H323-ID—H.323 ID of the endpoint. ■ Carrier—Carrier that is associated with the endpoint. ■ Max Calls—Maximum number of calls that the circuit can handle. ■ Available—Number of new calls that the circuit can handle currently.
<p>show gatekeeper endpoints [<i>alternates</i>]</p>	<p>To display the status of all registered endpoints for a gatekeeper, use the show gatekeeper endpoints command in privileged EXEC mode.</p> <p>The command has this keyword:</p> <ul style="list-style-type: none"> ■ alternates—(Optional) Displays information about alternate endpoints. All information that is normally included with this command is also displayed. <p>show gatekeeper endpoints field descriptions are as follows:</p>

Command	Description
	<ul style="list-style-type: none"> ■ CallsignalAddr—Call-signaling IP address of the endpoint. If the endpoint is also registered with an alias (or aliases), a list of all aliases that are registered for that endpoint should be listed on the line below. ■ Port—Call-signaling port number of the endpoint. ■ RASSignalAddr—RAS protocol IP address of the endpoint. ■ Port—RAS port number of the endpoint. ■ Zone Name—Zone name (gatekeeper ID) to which this endpoint is registered. ■ Type—Endpoint type (for example, terminal, gateway, or MCU). ■ F - S—The endpoint is statically entered from the alias command rather than being dynamically registered through RAS messages. ■ O—The endpoint, which is a gateway, has sent notification that it is nearly out of resources. ■ Voice Capacity Max.—Maximum number of channels available on the endpoint. ■ Avail.—Current number of channels available on the endpoint. ■ Total number of active registrations—Total number of endpoints that are registered with the gatekeeper.
<pre>show gatekeeper gw-type- prefix</pre>	<p>To display the gateway technology prefix table, use the show gatekeeper gw-type-prefix command in privileged EXEC mode.</p> <p>This command has no arguments or keywords.</p>
<pre>show gatekeeper performance statistics [zone [name zone-name]] [cumulative]</pre>	<p>To display information about the number of calls that are accepted and rejected and to find the number of endpoints that are sent to other gatekeepers, use the show gatekeeper performance statistics command in privileged EXEC mode.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ zone—(Optional) Zone statistics for the gatekeeper. ■ name—(Optional) Zone name or gatekeeper name. ■ zone-name—(Optional) Local zone name. ■ cumulative—(Optional) Total statistics that have been collected by the gatekeeper since the last reload. These values are not reset by the clear h323 gatekeeper statistics command. <p>show gatekeeper performance statistics field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ Full RRQs received—A full RRQ contains all registration information that is used to establish or change a registration. ■ Light RRQs received—A light RRQ contains abbreviated registration information that is used to maintain an existing registration.

Command	Description
<pre>show gatekeeper servers [<i>gkid</i>]</pre>	<p>To display a list of currently registered and statically configured triggers on a gatekeeper router, use the show gatekeeper servers command in EXEC mode.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>gkid</i>—(Optional) Local gatekeeper name to which this trigger applies. <p>show gatekeeper servers field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ GateKeeper GKTMP version—Version of Gatekeeper Transaction Message Protocol installed. ■ RRQ Priority—Registration priority. ■ Server-ID—Server ID name. ■ Server IP address—Server IP address. ■ Server type—Type of server. ■ Connection Status—Indicates whether the connection is active or inactive. ■ Trigger Information—Indicates which RAS messages that the Cisco IOS gatekeeper forwards to the external application. ■ REQUEST RRQ—Registration requests received. ■ RESPONSE RRQ—Registration responses received. ■ RESPONSE RCF—Response confirmations received. ■ RESPONSE RRJ—Response reject messages received.
<pre>show gatekeeper zone cluster</pre>	<p>To display the dynamic status of all local clusters, use the show gatekeeper zone cluster command in privileged EXEC mode.</p> <p>This command has no arguments or keywords.</p>
<pre>show gatekeeper zone prefix [<i>all</i>]</pre>	<p>To display the zone prefix table, use the show gatekeeper zone prefix command in privileged EXEC mode.</p> <p>The command has this keyword:</p> <ul style="list-style-type: none"> ■ all—(Optional) Displays the dynamic zone prefixes that are registered by each gateway. <p>show gatekeeper zone prefix field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ GK-NAME—Gatekeeper name. ■ E164-PREFIX—E.164 prefix and a dot that acts as a wildcard for matching each remaining number in the telephone number. ■ Dynamic GW-priority—Gateway that serves this E.164 prefix.

Command	Description
	<ul style="list-style-type: none"> ■ Gateway priority—A 0 value prevents the gatekeeper from using the gateway for that prefix. A value of 10 places the highest priority on the gateway. The default priority value for a dynamic gateway is 5.
<pre>show gatekeeper zone status</pre>	<p>To display the status of zones that are related to a gatekeeper, use the show gatekeeper zone status command in privileged EXEC mode.</p> <p>This command has no arguments or keywords.</p> <p>show gatekeeper zone status field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ GK name—Gatekeeper name (also known as the zone name), which is truncated after 12 characters in the display. ■ Domain Name—Domain with which the gatekeeper is associated. ■ RAS Address— RAS protocol address of the gatekeeper. ■ FLAGS—Displays this information: <ul style="list-style-type: none"> ■ S = static (CLI-configured, not DNS-discovered) ■ L = local ■ R = remote ■ MAX-BW—Maximum bandwidth for the zone, in kbps. ■ CUR-BW—Current bandwidth in use, in kbps. ■ SUBNET ATTRIBUTES—List of subnets that are controlled by the local gatekeeper. ■ PROXY USAGE CONFIGURATION—Inbound and outbound proxy policies as configured for the local gatekeeper (or zone).
<pre>tech-prefix number</pre>	<p>To specify that a particular technology prefix be prepended to the destination pattern of a specific dial peer, use the tech-prefix command in dial-peer configuration mode. To disable the defined technology prefix for this dial peer, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ <i>number</i>—Defines the numbers that are used as the technology prefix. Each technology prefix can contain up to 11 characters. Although not strictly necessary, a pound (#) symbol is frequently used as the last character in a technology prefix. Valid characters are 0 through 9, the pound (#) symbol, and the asterisk (*).
<pre>zone local gatekeeper-name domain-name [ras-IP- address] [invia inbound gatekeeper outvia outbound gatekeeper [enable-intrazone]]</pre>	<p>To specify a zone that is controlled by a gatekeeper, use the zone local command in gatekeeper configuration mode. To remove a zone that is controlled by a gatekeeper, use the no form of this command.</p> <p>The command has these keywords and arguments:</p>

Command	Description
	<ul style="list-style-type: none"> ■ <i>gatekeeper-name</i>—Gatekeeper name or zone name. This is usually the fully domain-qualified host name of the gatekeeper. For example, if the <i>domain-name</i> is cisco.com, the <i>gatekeeper-name</i> might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the <i>gatekeeper-name</i> for each zone should be some unique mnemonic string. ■ <i>domain-name</i>—The domain name that is served by this gatekeeper. ■ <i>ras-IP-address</i>—(Optional) 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. <p>Note: Setting this address for one local zone makes it the address that is used for all local zones.</p> <ul style="list-style-type: none"> ■ <i>invia</i>—Specifies the gatekeeper for calls that are entering this zone. ■ <i>inbound gatekeeper</i>—Name of the inbound gatekeeper. ■ <i>outvia</i>—Specifies the gatekeeper for calls that are leaving this zone. ■ <i>outbound gatekeeper</i>—Name of the outbound gatekeeper. ■ <i>enable-intrazone</i>—Forces all intrazone calls to use the via-gatekeeper.
<pre>zone prefix gatekeeper- name e164-prefix [blast seq] [gw-priority priority gw-alias [gw-alias, ...]]</pre>	<p>To add a prefix to the gatekeeper zone list, use the zone prefix command in gatekeeper configuration mode. To remove knowledge of a zone prefix, use the no form of this command with the gatekeeper name and prefix. To remove the priority assignment for a specific gateway, use the no form of this command with the gw-priority option.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ <i>gatekeeper-name</i>—Name of a local or remote gatekeeper, which must have been defined by using the zone local or zone remote command. ■ <i>e164-prefix</i>—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 seven numbers. <p>Note: Although a dot that represents each digit in an E.164 address is the preferred configuration method, you can also enter an asterisk (*) to match any number of digits.</p> <ul style="list-style-type: none"> ■ blast—(Optional) If you list multiple hopoffs, this keyword indicates that the LRQs should be sent simultaneously to the gatekeepers based on the order in which the gatekeepers were listed. The default is seq. ■ seq—(Optional) If you list multiple hopoffs, this keyword indicates that the LRQs should be sent sequentially to the gatekeepers based on the order in which the gatekeepers were listed. The default is seq.

Command	Description
	<ul style="list-style-type: none"> ■ gw-priority <i>pri-0-to-10 gw-alias</i>—(Optional) Defines how the gatekeeper selects gateways in its local zone for calls to numbers that begin with the prefix <i>e164-prefix</i>. Do not use this option to set priority levels for a prefix that is assigned to a remote gatekeeper. <p>The range is from 0 to 10, where 0 prevents the gatekeeper from using the gateway <i>gw-alias</i> for that prefix and 10 places the highest priority on gateway <i>gw-alias</i>. The default is 5.</p> <p>To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the <i>pri-0-to-10</i> value.</p> <ul style="list-style-type: none"> ■ gw-alias—(Optional) The alias is the H.323 ID of a gateway that is registered or will register with the gatekeeper. This alias is set on the gateway with the h323-gateway voip h.323-id command.
<pre>zone remote other- gatekeeper-name other- domain-name other- gatekeeper-ip-address [port-number] [cost cost- value [priority priority- value]] [foreign-domain] [invia inbound gatekeeper] [outvia outbound gatekeeper] no zone remote other- gatekeeper-name other- domain-name other- gatekeeper-ip-address [port-number] [cost cost- value [priority priority- value]] [foreign-domain] [invia inbound gatekeeper] [outvia outbound gatekeeper]</pre>	<p>To statically specify a remote zone if DNS is unavailable or undesirable, use the zone remote command in gatekeeper configuration mode. To remove the remote zone, use the no form of this command.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ other-gatekeeper-name—Name of the remote gatekeeper. ■ other-domain-name—Domain name of the remote gatekeeper. ■ other-gatekeeper-ip-address—IP address of the remote gatekeeper. ■ port-number—(Optional) RAS signaling port number for the remote zone. The range is from 1 to 65535. If the value is not set, the default is the well-known RAS port number 1719. ■ cost cost-value—(Optional) Cost of the zone. The range is from 1 to 100. The default is 50. ■ priority priority-value—(Optional) Priority of the zone. The range is from 1 to 100. The default is 50. ■ foreign-domain—(Optional) Indicates that the cluster is in a different administrative domain. ■ invia—(Optional) Specifies the gatekeeper for calls that are entering this zone. ■ inbound gatekeeper—(Optional) Name of the inbound gatekeeper. ■ outvia—(Optional) Specifies the gatekeeper for calls that are leaving this zone. ■ outbound gatekeeper—(Optional) Name of outbound gatekeeper.

Job Aids

There are no job aids for this lab activity.

Task 1: Configure a Gatekeeper at BR2

Further discussions with Armstrong Snow Shovel reveal that the company is still concerned that IP WAN bandwidth will be used at the expense of voice quality and data flow. The company is also concerned that, as the firm grows, it will need a centralized facility for E.164 address resolution. This need can be accomplished by deploying gatekeepers at HQ and at BR2. These gatekeepers can be used to resolve calls between these locations.

Configure two zones, HQ and BR2, and configure appropriate dial-plan information for the gatekeepers to resolve calls between HQ and BR2. Configure CAC to allow one call between BR2 and HQ. The technology prefix should be set to 1#*. The domain for Armstrong Snow Shovel is ASC.com.

In this task you will first configure BR2. In the next task you will configure HQ.

Activity Procedure

Complete these steps:

- Step 1** Configure the H.323 gatekeeper at BR2. The gatekeeper can be accessed from the terminal server. The host name is BR2GK.
- Step 2** Configure the gatekeeper to support E.164 address resolution and CAC. Set the CAC interzone bandwidth to support one call.
- Step 3** Configure BR2 to register with BR2GK. Modify the existing VoIP dial peers to use the gatekeeper for number resolution.

Activity Verification

You have completed this task when you attain these results:

- You can verify that the gateway at BR2 registers with the gatekeeper at BR1 and two zones appear in the configuration of the gatekeeper: a local zone and a remote zone.
- You can test the dial-plan resolution and CAC by placing calls from HQ to BR2.

Task 2: Configure a Gatekeeper at HQ

The configuration tasks at HQ are similar to the configuration at BR2.

Configure HQ as an H.323 gatekeeper.

- Step 1** Configure the Cisco CallManager cluster so that it registers with the gatekeeper. Accomplish this step by configuring a gatekeeper-controlled intercluster trunk. Make sure that you use an MTP. Set the device pool to “HQ” and the calling search space to “HQ_Internal.”
- Step 2** Add the intercluster trunk that was defined in Step 1 to a route group that is named “HQ-BR2.” Modify the existing BR2 route list to include the HQ-BR2 route group. Make sure that the HQ-BR2 route group is the first route group that is selected.
- Step 3** Configure the gatekeeper to support E.164 address resolution and CAC. Set the CAC bandwidth to allow one call.

Activity Verification

You have completed this task when you attain these results:

- You can verify that Cisco CallManager registers with the gatekeeper at HQ.
- You can test the dial-plan resolution and CAC by placing calls from HQ to BR2.

Lab 5-1 Answer Key: Configuring Gatekeepers

When you complete this activity, your H.323 gatekeeper will be similar to the results here, with differences that are specific to your device or workgroup:

Task 1 Solution

- Step 1** Configure the BR2GK gatekeeper with a local zone BR2 and a remote zone HQ. Type these commands on BR2GK:

```
gatekeeper
zone local BR2 ASC.com
zone remote HQ ASC.com 10.1.10.1
no shutdown
```

- Step 2** Configure three zone prefixes: 2... and 3... should be handled by the HQ zone and 4... should be handled by the BR2 zone. Configure the tech prefix and the bandwidth for CAC. Type these commands on BR2GK in gatekeeper configuration mode:

```
zone prefix BR2 4...
zone prefix HQ 2...
zone prefix HQ 3...
gw-type-prefix 1#* default-technology
bandwidth interzone zone BR2 80
```

- Step 3** Configure BR2 to register with BR2GK and modify the VoIP dial peers to use the gatekeeper. Type these commands on BR2:

```
interface fastethernet 0/0.30
h323-gateway voip id BR2 ipaddr 10.3.30.30
h323-gateway voip h323-id BR2
h323-gateway voip tech-prefix 1#
dial-peer voice 2000 voip
session target ras
dial-peer voice 3000 voip
session target ras
```

Task 2 Solution

- Step 1** Configure the HQ gatekeeper with a local zone HQ and a remote zone BR2. Type these commands on HQ:

```
gatekeeper
zone local HQ ASC.com
zone remote BR2 ASC.com 10.3.30.30
no shutdown
```

- Step 2** Configure three zone prefixes: 2... and 3... should be handled by the HQ zone and 4... should be handled by the BR2 zone. Configure the tech prefix and the bandwidth for CAC. Type these commands on BR2GK in gatekeeper configuration mode:

```
zone prefix BR2 4...
zone prefix HQ 2...
zone prefix HQ 3...
gw-type-prefix 1#* default-technology
bandwidth interzone zone HQ 80
```

Task 3 Solution

Configure Cisco CallManager to register with the HQ gatekeeper. Complete these tasks:

- Step 1** Add a gatekeeper to Cisco CallManager under Device > gatekeeper and add the RAS IP address 10.1.10.1 of the gatekeeper.
- Step 2** Add a gatekeeper-controlled intercluster trunk.
- Step 3** Name the intercluster trunk “HQ-BR2.” (Make sure that you select an MTP.)
- Step 4** Set the device pool to “HQ” and the calling search space to “HQ_Internal.”
- Step 5** Add a route group that is named “HQ-BR2.”
- Step 6** Place the newly created intercluster trunk in this route group.
- Step 7** Modify the existing route list BR2 to include the newly create route group.
- Step 8** Add the HQ-BR2 route group to this route list as the first route group member.
- Step 9** To verify that calls from HQ to BR2 are resolved by the gatekeeper, enter **debug ras** on HQ.
- Step 10** Place a call from 2001 to 4001 and verify that RAS messages are seen on HQ.

Lab 5-2: Configuring Directory Gatekeepers

Complete this lab activity to practice what you learned in the related module.

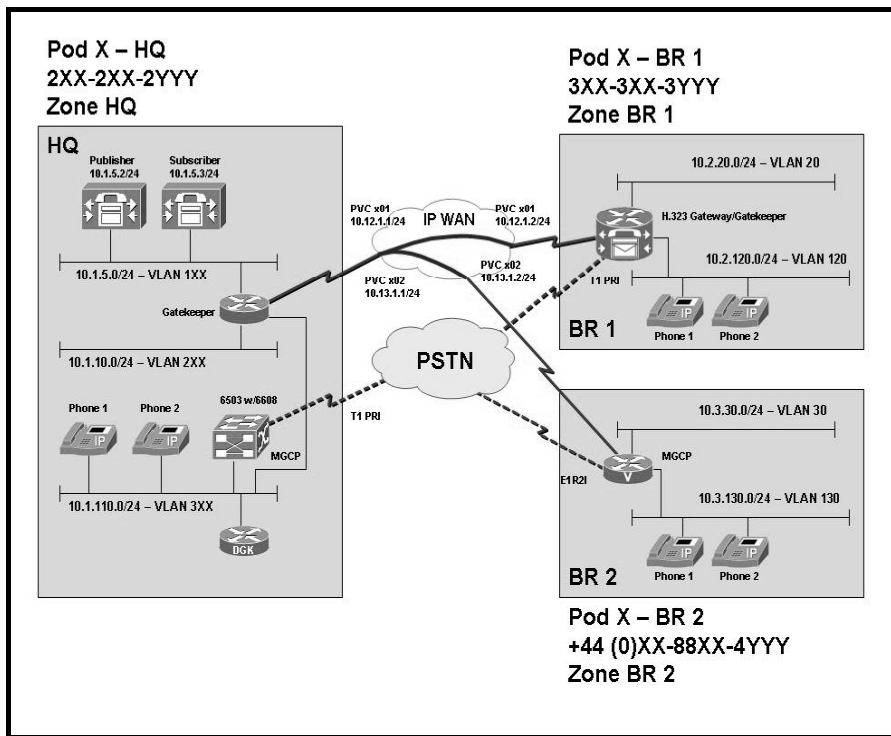
Activity Objective

In this activity, you will implement a directory gatekeeper to provide hierarchical dial-plan resolution to two gatekeeper zones. After completing this activity, you will be able to meet this objective:

- Create a dial-plan resolution hierarchy through the implementation of a directory gatekeeper

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Student Pods

The student pod equipment requirements are as follows:

- Six Cisco IP phones, which can be any model except for 7920. The IP Phones require power from either an in-line power switch or external power bricks.
- One Cisco router with one 10/100 Ethernet interface, one T1 serial interface, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one T1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one E1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with one 10/100 Ethernet interface and Cisco IOS Release 12.3(11)T3.
- One Cisco Catalyst 3550 switch for each branch location or one internal EtherSwitch module for the router.
- One Cisco Catalyst 6500 switch with a 10/100 Ethernet switch module and one WS-X6608 gateway module for the HQ location.
- One Cisco CallManager publisher and subscriber.

Network Core

The network core equipment requirements are as follows:

- One Cisco router to provide Frame Relay or ATM support to an IP WAN to connect the HQ with BR1 and BR2.
- One Cisco CallManager and one Cisco router configured as an MGCP gateway to provide the functionality of the PSTN to all locations.

Command List

The table describes the commands that are used in this activity.

Directory Gatekeeper Commands

Command	Description
<pre>bandwidth {interzone total session} {default zone zone-name} bandwidth-size</pre>	<p>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 the maximum aggregate bandwidth, use the no form of this command.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ 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 that is allowed in the zone. ■ session—Maximum bandwidth that is 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 10000000. For session, the range is from 1 to 5000.
<pre>debug gatekeeper gup {events asn1}</pre>	<p>To display the GUP events or ASN.1 details, use the debug gatekeeper gup command in privileged EXEC mode. To disable debugging output, use the no form of this command.</p> <p>The command has these keywords:</p> <ul style="list-style-type: none"> ■ events—Displays a message whenever a GUP announcement is sent or received. GUP is the protocol that is used between individual gatekeepers in a cluster; GUP keeps all the gatekeepers synchronized with all endpoints that are registered on the cluster. ■ asn1—ASN.1 library. ASN.1 is an ITU standard for protocol syntax and message encoding. Entering this keyword causes a packet dump of all GUP announcement messages.
<pre>debug gatekeeper load {events}</pre>	<p>To display gatekeeper load-balancing debug events, use the debug gatekeeper load command in privileged EXEC mode. To disable debugging output, use the no form of this command.</p> <p>The command has this keyword:</p> <ul style="list-style-type: none"> ■ events—Displays a message whenever a load-balancing message is sent or received.

Command	Description
<code>debug gatekeeper server</code>	<p>To trace all the message exchanges between the Cisco IOS gatekeeper and the external applications, use the debug gatekeeper server command in privileged EXEC mode. To disable debugging output, use the no form of this command.</p> <p>This command has no arguments or keywords.</p>
<code>gatekeeper</code>	Enters gatekeeper configuration mode.
<code>gw-type-prefix type-prefix</code> <code>[[hopoff gkid1] [hopoff gkid2] [hopoff gkidn] [seq blast]] [default-technology] [[gw ipaddr ipaddr [port]]]</code>	<p>To configure a technology prefix in the gatekeeper, use the gw-type-prefix command in gatekeeper configuration mode. To remove the technology prefix, use the no form of this command.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ type-prefix—The technology prefix is recognized and is stripped before you check for the zone prefix. It is strongly recommended that you select technology prefixes that do not lead to ambiguity with zone prefixes. Do this by using the # character to terminate technology prefixes, for example, 3#. ■ hopoff gkid—(Optional) Use this option to specify the gatekeeper where the call is to hop off, regardless of the zone prefix in the destination address. The <i>gkid</i> argument refers to a gatekeeper that was previously configured using the zone local or zone remote command. You can enter this keyword and argument multiple times to configure redundant gatekeepers for a given technology prefix. ■ seq blast—(Optional) If you list multiple hopoffs, these keywords indicate that the LRQs should be sent sequentially or simultaneously (blast) to the gatekeepers according to the order in which the gatekeepers were listed. The default is to send them sequentially. ■ default-technology—(Optional) Gateways that register with this prefix option are used as the default for routing any addresses that are otherwise unresolved. ■ gw ipaddr ipaddr [port]—(Optional) Use this option to indicate that the gateway is incapable of registering technology prefixes. When it registers, it adds the gateway to the group for this type of prefix, just as if it had sent the technology prefix in its registration. This parameter can be repeated to associate more than one gateway with a technology prefix.
<code>no shutdown</code>	Activates the gatekeeper.
<code>show gatekeeper calls</code>	<p>To display the status of each ongoing call of which a gatekeeper is aware, use the show gatekeeper calls command in privileged EXEC mode.</p> <p>This command has no arguments or keywords.</p> <p>show gatekeeper calls field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ LocalCallID —Identification number of the call. ■ Age(secs)—Age of the call, in seconds. ■ BW(Kbps)—Bandwidth in use, in kilobytes per second.

Command	Description
	<ul style="list-style-type: none"> ■ Ends—Role of each endpoint (terminal, gateway, or proxy) in the call (originator, target, or proxy) and the call-signaling and RAS protocol address. ■ Alias—H.323 ID or e-mail ID of the endpoint. ■ E.164Addr—E.164 address of the endpoint. ■ CallSignalAddr—Call-signaling IP address of the endpoint. ■ Port—Call-signaling port number of the endpoint. ■ RASSignalAddr—RAS IP address of the endpoint. ■ Port—RAS port number of the endpoint.
<pre>show gatekeeper circuits [begin exclude include] <i>expression</i></pre>	<p>To display the circuit information on a gatekeeper, use the show gatekeeper circuits command in privileged EXEC mode.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ begin—(Optional) Displays all circuits, beginning with the line that contains the expression. ■ exclude—(Optional) Displays all circuits, excluding those that contain the expression. ■ include—(Optional) Displays all circuits, including those that contain the expression. ■ expression—(Optional) Word or phrase that is used to determine what lines are displayed. <p>show gatekeeper circuits field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ Circuit—Name of each circuit that is connected to the gatekeeper. ■ Endpoint—Name of each H.323 endpoint. ■ Max Calls—Maximum number of calls that the circuit can handle. ■ Avail Calls—Number of new calls that the circuit can handle at the current time. ■ Resources—Indicates whether circuit resources have exceeded the defined threshold limits. The endpoint resource-threshold command defines these thresholds. ■ Zone—Zone that supports the endpoint. The zone circuit-id command assigns a zone to an endpoint. ■ Total Endpoints—Total number of endpoints that are supported by the circuit. ■ Total Zones—Total number of zones that are supported by the circuit.
<pre>show gatekeeper endpoint circuits [begin exclude include] <i>expression</i></pre>	<p>To display the information of all registered endpoints and carriers or trunk groups for a gatekeeper, use the show gatekeeper endpoint circuits command in privileged EXEC mode.</p> <p>The command has these keywords and arguments:</p>

Command	Description
	<ul style="list-style-type: none"> ■ begin—(Optional) Displays all circuits, beginning with the line that contains the expression. ■ exclude—(Optional) Displays all circuits, excluding those that contain the expression. ■ include—(Optional) Displays all circuits, including those that contain the expression. ■ expression—(Optional) Word or phrase that is used to determine what lines are displayed. <p>show gatekeeper endpoint circuits field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ CallsignalAddr—Call-signaling IP address of the endpoint. If the endpoint is also registered with an alias, a list of all aliases that are registered for that endpoint should be listed on the line below. ■ Port—Call-signaling port number of the endpoint. ■ RASSignalAddr—RAS IP address of the endpoint. ■ Port—RAS port number of the endpoint. ■ Zone Name—Zone name (gatekeeper ID) that this endpoint registered in. ■ Type—Endpoint type (for example, terminal, gateway, or MCU). ■ Flags - S—The endpoint is statically entered from the alias command rather than being dynamically registered through RAS messages. ■ O—The endpoint, which is a gateway, has sent notification that it is nearly out of resources. ■ E164-ID—E.164 ID of the endpoint. ■ H323-ID—H.323 ID of the endpoint. ■ Carrier—Carrier that is associated with the endpoint. ■ Max Calls—Maximum number of calls that the circuit can handle. ■ Available—Number of new calls that the circuit can handle currently.
<p>show gatekeeper endpoints [alternates]</p>	<p>To display the status of all registered endpoints for a gatekeeper, use the show gatekeeper endpoints command in privileged EXEC mode.</p> <p>The command has this keyword:</p> <ul style="list-style-type: none"> ■ alternates—(Optional) Displays information about alternate endpoints. All information that is normally included with this command is also displayed. <p>show gatekeeper endpoints field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ CallsignalAddr—Call-signaling IP address of the endpoint. If the endpoint is also registered with an alias (or aliases), a list of all aliases that are registered for that endpoint should be listed on the line below. ■ Port—Call-signaling port number of the endpoint.

Command	Description
	<ul style="list-style-type: none"> ■ RASSignalAddr—RAS protocol IP address of the endpoint. ■ Port—RAS port number of the endpoint. ■ Zone Name—Zone name (gatekeeper ID) to which this endpoint is registered. ■ Type—Endpoint type (for example, terminal, gateway, or MCU). ■ F - S—The endpoint is statically entered from the alias command rather than being dynamically registered through RAS messages. ■ O—The endpoint, which is a gateway, has sent notification that it is nearly out of resources. ■ Voice Capacity Max.—Maximum number of channels available on the endpoint. ■ Avail.—Current number of channels available on the endpoint. ■ Total number of active registrations—Total number of endpoints that are registered with the gatekeeper.
<pre>show gatekeeper gw-type- prefix</pre>	<p>To display the gateway technology prefix table, use the show gatekeeper gw-type-prefix command in privileged EXEC mode.</p> <p>This command has no arguments or keywords.</p>
<pre>show gatekeeper performance statistics [zone [name zone-name]] [cumulative]</pre>	<p>To display information about the number of calls that are accepted and rejected and to find the number of endpoints that are sent to other gatekeepers, use the show gatekeeper performance statistics command in privileged EXEC mode.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ zone—(Optional) Zone statistics for the gatekeeper. ■ name—(Optional) Zone name or gatekeeper name. ■ zone-name—(Optional) Local zone name. ■ cumulative—(Optional) Total statistics that have been collected by the gatekeeper since the last reload. These values are not reset by the clear h323 gatekeeper statistics command. <p>show gatekeeper performance statistics field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ Full RRQs received—A full RRQ contains all registration information that is used to establish or change a registration. ■ Light RRQs received—A light RRQ contains abbreviated registration information that is used to maintain an existing registration.
<pre>show gatekeeper servers [<i>gkid</i>]</pre>	<p>To display a list of currently registered and statically configured triggers on a gatekeeper router, use the show gatekeeper servers command in EXEC mode.</p>

Command	Description
	<p>The command has this argument:</p> <ul style="list-style-type: none"> ■ gkid—(Optional) Local gatekeeper name to which this trigger applies. <p>show gatekeeper servers field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ GateKeeper GKTMP version—Version of Gatekeeper Transaction Message Protocol installed. ■ RRQ Priority—Registration priority. ■ Server-ID—Server ID name. ■ Server IP address—Server IP address. ■ Server type—Type of server. ■ Connection Status—Indicates whether the connection is active or inactive. ■ Trigger Information—Indicates which RAS messages that the Cisco IOS gatekeeper forwards to the external application. ■ REQUEST RRQ—Registration requests received. ■ RESPONSE RRQ—Registration responses received. ■ RESPONSE RCF—Response confirmations received. ■ RESPONSE RRJ—Response reject messages received.
<p>show gatekeeper zone cluster</p>	<p>To display the dynamic status of all local clusters, use the show gatekeeper zone cluster command in privileged EXEC mode.</p> <p>This command has no arguments or keywords.</p>
<p>show gatekeeper zone prefix [all]</p>	<p>To display the zone prefix table, use the show gatekeeper zone prefix command in privileged EXEC mode.</p> <p>The command has this keyword:</p> <ul style="list-style-type: none"> ■ all—(Optional) Displays the dynamic zone prefixes that are registered by each gateway. <p>show gatekeeper zone prefix field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ GK-NAME—Gatekeeper name. ■ E164-PREFIX—E.164 prefix and a dot that acts as a wildcard for matching each remaining number in the telephone number. ■ Dynamic GW-priority—Gateway that serves this E.164 prefix. ■ Gateway priority. A 0 value prevents the gatekeeper from using the gateway for that prefix. A value of 10 places the highest priority on the gateway. The default priority value for a dynamic gateway is 5.
<p>show gatekeeper zone status</p>	<p>To display the status of zones that are related to a gatekeeper, use the show gatekeeper zone status command in privileged EXEC mode.</p>

Command	Description
	<p>This command has no arguments or keywords.</p> <p>show gatekeeper zone status field descriptions are as follows:</p> <ul style="list-style-type: none"> ■ GK name—Gatekeeper name (also known as the zone name), which is truncated after 12 characters in the display. ■ Domain Name—Domain with which the gatekeeper is associated. ■ RAS Address—RAS protocol address of the gatekeeper. ■ FLAGS—Displays this information: <ul style="list-style-type: none"> ■ S = static (CLI-configured, not DNS-discovered) ■ L = local ■ R = remote ■ MAX-BW—Maximum bandwidth for the zone, in kbps. ■ CUR-BW—Current bandwidth in use, in kbps. ■ SUBNET ATTRIBUTES—List of subnets that are controlled by the local gatekeeper. ■ PROXY USAGE CONFIGURATION—Inbound and outbound proxy policies as configured for the local gatekeeper (or zone).

Command	Description
<pre>tech-prefix number</pre>	<p>To specify that a particular technology prefix be prepended to the destination pattern of a specific dial peer, use the tech-prefix command in dial-peer configuration mode. To disable the defined technology prefix for this dial peer, use the no form of this command.</p> <p>The command has this argument:</p> <ul style="list-style-type: none"> ■ number—Defines the numbers that are used as the technology prefix. Each technology prefix can contain up to 11 characters. Although not strictly necessary, a pound (#) symbol is frequently used as the last character in a technology prefix. Valid characters are 0 through 9, the pound (#) symbol, and the asterisk (*).
<pre>zone local gatekeeper-name domain-name [ras-IP- address] [invia inbound gatekeeper outvia outbound gatekeeper [enable-intrazone]]</pre>	<p>To specify a zone controlled by a gatekeeper, use the zone local command in gatekeeper configuration mode. To remove a zone controlled by a gatekeeper, use the no form of this command.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ gatekeeper-name—Gatekeeper name or zone name. This name is usually the fully domain-qualified host name of the gatekeeper. For example, if the <i>domain-name</i> is cisco.com, the <i>gatekeeper-name</i> might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the <i>gatekeeper-name</i> for each zone should be some unique mnemonic string. ■ domain-name—The domain name that is served by this gatekeeper. ■ ras-IP-address—(Optional) 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. <p>Note: Setting this address for one local zone makes it the address that is used for all local zones.</p> <ul style="list-style-type: none"> ■ invia—(Optional) Specifies the gatekeeper for calls that are entering this zone. ■ inbound gatekeeper—(Optional) Name of the inbound gatekeeper. ■ outvia—(Optional) Specifies the gatekeeper for calls that are leaving this zone. ■ outbound gatekeeper—(Optional) Name of the outbound gatekeeper. ■ enable-intrazone—(Optional) Forces all intrazone calls to use the via-gatekeeper.
<pre>zone prefix gatekeeper- name e164-prefix [blast seq] [gw-priority priority gw-alias [gw-alias, ...]]</pre>	<p>To add a prefix to the gatekeeper zone list, use the zone prefix command in gatekeeper configuration mode. To remove knowledge of a zone prefix, use the no form of this command with the gatekeeper name and prefix. To remove the priority assignment for a specific gateway, use the no form of this command with the gw-priority option.</p>

Command	Description
	<p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ gatekeeper-name—Name of a local or remote gatekeeper, which must have been defined by using the zone local or zone remote command. ■ e164-prefix—E.164 prefix in standard form followed by dots (.). Each dot represents a number in the E.164 address. For example, 212..... is matched by 212 and any seven numbers. <p>Note: Although a dot that represents each digit in an E.164 address is the preferred configuration method, you can also enter an asterisk (*) to match any number of digits.</p> <ul style="list-style-type: none"> ■ blast—(Optional) If you list multiple hopoffs, this keyword indicates that the LRQs should be sent simultaneously to the gatekeepers based on the order in which the gatekeepers were listed. The default is seq. ■ seq—(Optional) If you list multiple hopoffs, this keyword indicates that the LRQs should be sent sequentially to the gatekeepers based on the order in which the gatekeepers were listed. The default is seq. ■ gw-priority pri-0-to-10 gw-alias—(Optional) Defines how the gatekeeper selects gateways in its local zone for calls to numbers that begin with the prefix e164-prefix. Do not use this option to set priority levels for a prefix that assigned to a remote gatekeeper. <p>The range is from 0 to 10, where 0 prevents the gatekeeper from using the gateway <i>gw-alias</i> for that prefix and 10 places the highest priority on gateway <i>gw-alias</i>. The default is 5.</p> <p>To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the <i>pri-0-to-10</i> value.</p> <ul style="list-style-type: none"> ■ gw-alias—(Optional) This alias is the H.323 ID of a gateway that is registered or will register with the gatekeeper. This alias is set on the gateway with the <code>h323-gateway voip h.323-id</code> command.
<pre> zone remote other- gatekeeper-name other- domain-name other- gatekeeper-ip-address [port-number] [cost cost- value [priority priority- value]] [foreign-domain] [invia inbound gatekeeper] [outvia outbound gatekeeper] no zone remote other- gatekeeper-name other- domain-name other- gatekeeper-ip-address [port-number] [cost cost- value [priority priority- value]] [foreign-domain] [invia inbound gatekeeper] </pre>	<p>To statically specify a remote zone if DNS is unavailable or undesirable, use the zone remote command in gatekeeper configuration mode. To remove the remote zone, use the no form of this command.</p> <p>The command has these keywords and arguments:</p> <ul style="list-style-type: none"> ■ other-gatekeeper-name—Name of the remote gatekeeper. ■ other-domain-name—Domain name of the remote gatekeeper. ■ other-gatekeeper-ip-address—IP address of the remote gatekeeper. ■ port-number—(Optional) RAS signaling port number for the remote zone. Range is from 1 to 65535. If the value is not set, the default is the well-known RAS port number 1719.

Command	Description
<pre> [outvia outbound gatekeeper]</pre>	<ul style="list-style-type: none"> ■ cost cost-value—(Optional) Cost of the zone. The range is from 1 to 100. The default is 50. ■ priority priority-value—(Optional) Priority of the zone. The range is from 1 to 100. The default is 50. ■ foreign-domain—(Optional) Indicates that the cluster is in a different administrative domain. ■ invia—(Optional) Specifies the gatekeeper for calls that are entering this zone. ■ inbound gatekeeper—(Optional) Name of the inbound gatekeeper. ■ outvia—(Optional) Specifies the gatekeeper for calls that are leaving this zone. ■ outbound gatekeeper—(Optional) Name of the outbound gatekeeper.

Job Aids

There are no job aids for this lab activity.

Task 1: Configure the Directory Gatekeeper

Armstrong Snow Shovel is interested in how to centralize call resolution in the network so that the telephony system can scale. The company is still concerned that a single IP WAN outage could cause a serious problem. In response, you have again shown the company your lab activity where you have a test network set up that resembles the Armstrong Snow Shovel network. To demonstrate centralized call resolution, you need to implement a directory gatekeeper.

Activity Procedure

Complete this step:

- Step 1** You have added another router to perform the tasks of a directory gatekeeper. Configure it to be a directory gatekeeper with a zone name of DGK. Make sure that the interzone bandwidth that you set in the previous lab is maintained.

Activity Verification

You have completed this task when you attain this result:

- You can verify that calls can be placed to and from each location.

Lab 5-2 Answer Key: Configuring Directory Gatekeepers

When you complete this activity, your zone gatekeeper and directory gatekeeper configurations will be similar to the results here, with differences that are specific to your device or workgroup:

Task 1 Solution

In the directory gatekeeper you will need to configure one local zone and two remote zones. Type these commands to complete this task:

```
zone local DGK ASC.com
zone remote HQ ASC.com 10.1.10.1
```

The second of these two commands enables the directory gatekeeper to know where to send calls that have a destination prefix that is associated with the HQ zone. When you press the Enter key, the default port 1719 will be added to this command statement.

The next command enables the directory gatekeeper to know where to send calls that have a destination prefix that is associated with the BR2 zone. When you press the Enter key, the default port 1719 will be added to this command statement.

```
zone remote BR2 ASC.com 10.3.30.30
```

Next, you will need to configure the remote prefixes in the directory gatekeeper. Type these commands to accomplish this task:

```
zone prefix HQ 2...
zone prefix HQ 3...
```

These two commands may appear to be confusing, but the HQ zone covers both HQ and BR1 and is controlled by the Cisco CallManager. Thus, in order for the directory gatekeeper to learn the prefixes for this zone, these commands are required.

The next command allows the gatekeeper to learn the prefix for the BR2 zone:

```
zone prefix BR2 4...
```

The next command is the command that allows the directory gatekeeper to function as a relay. Without this command, incoming LRQs would not be forwarded to other remote gatekeepers to resolve a location request.

```
lrq forward-queries
```

This command enables the gatekeeper on the router:

```
no shut
```

Now the remote gatekeepers need to have their configurations modified to work with the directory gatekeeper.

Here is the output for the BR2 gatekeeper:

```
gatekeeper
zone local BR2 ASC.com
zone remote DGK ASC.com 10.1.10.10
zone prefix BR2 4...
zone prefix DGK *
gw-type-prefix 1#* default-technology
no shut
```

You will notice that the **zone remote** command now points to the directory gatekeeper and not to HQ. Also notice that the zone prefix for DGK is a *. This situation causes the BR2 gatekeeper to send every request that it cannot resolve to the 4... range to the directory gatekeeper. The IP address that is associated with **zone remote DGK ASC.com 10.1.10.10** is the IP address of the Ethernet interface on the directory gatekeeper. The **gw-type-prefix 1#* default-technology** command provides the technology prefix between the gatekeeper and the BR2 gateway. For this to operate correctly, these values must match, but you need to be careful because the gateway does not use the same syntax. The gateway uses 1# and the gatekeeper uses 1#*. They are equivalent but different.

The configuration for the HQ gatekeeper is as follows.

```
gatekeeper
zone local HQ ASC.com
zone remote DGK ASC.com 10.1.10.10
zone prefix HQ 2...
zone prefix HQ 3...
zone prefix DGK *
gw-type-prefix 1#* default-technology
no shut
```

The command syntax is similar to the BR2 gatekeeper with the exception of the additional zone prefix for the HQ zone. Remember, this zone covers both the HQ and BR1 locations, so both directory ranges are required.

Lab 6-1: Comprehensive Lab

Complete this lab activity to practice what you learned in the related module.

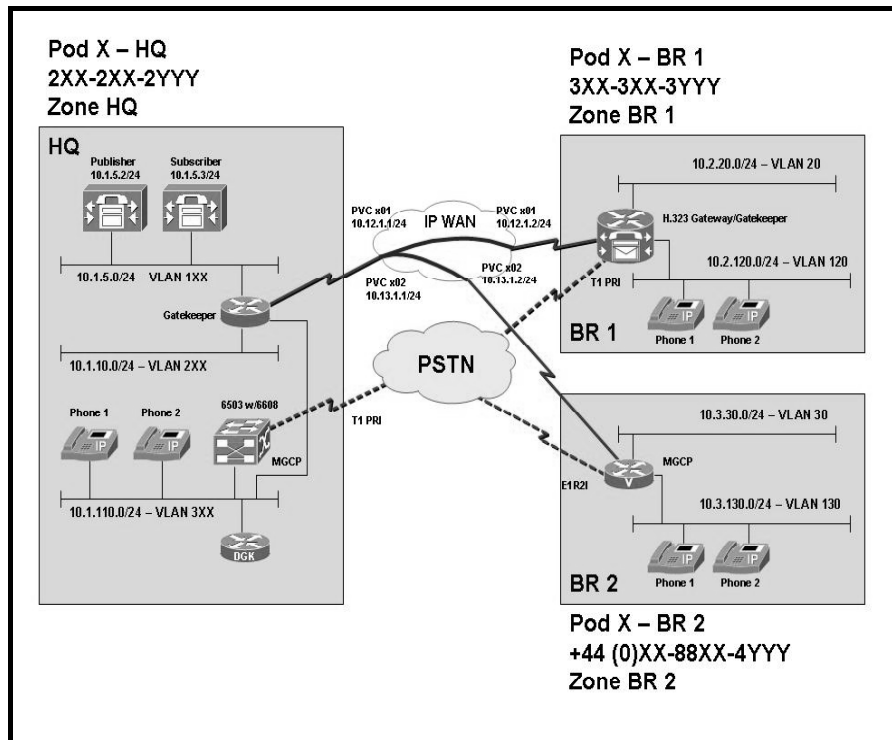
Activity Objective

In this activity, you will use all of the topics that have been covered in this course to create a comprehensive IP telephony solution. After completing this activity, you will be able to meet these objectives:

- Configure various gateway types
- Configure digit manipulation
- Create a dial plan with COR
- Deploy SRST
- Deploy DSP resources
- Implement TCL scripts
- Configure gatekeepers

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that are required to complete this activity:

Student Pods

The student pod equipment requirements are as follows:

- Six Cisco IP Phones, which can be any model except for 7920. The IP Phones require power from either an in-line power switch or external power bricks.
- One Cisco router with one 10/100 Ethernet interface, one T1 serial interface, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one T1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with two 10/100 Ethernet interfaces, one T1 serial interface, one E1 voice module, and Cisco IOS Release 12.3(11)T3.
- One Cisco router with one 10/100 Ethernet interface and Cisco IOS Release 12.3(11)T3.
- One Cisco Catalyst 3550 switch or one internal EtherSwitch module for the router.
- One Cisco Catalyst 6500 switch with one 10/100 Ethernet switch module and one WS-X6608 gateway module for the HQ location.
- One Cisco CallManager publisher and subscriber.

Network Core

The network core equipment requirements are as follows:

- One Cisco router to provide Frame Relay or ATM support to an IP WAN to connect the HQ with BR1 and BR2.
- One Cisco CallManager and one Cisco router configured as an MGCP gateway to provide the functionality of the PSTN to all locations.

Job Aids

These job aids are available to help you complete the lab activity.

Lab 6-1 Job Aids

Locations	Dial-Plan Range
HQ	2XX-2XX-2YYY
BR1	3XX-3XX-3YYY
BR2	+44 (0) XX-88XX-4YYY
Domain name	bigrockind.com

Note The numbering plan will use your pod number expressed in two digits for the XX portion of the plan. For example, if your pod is number 2, it is expressed as 02 in the numbering plan.

Type	Dial-Plan Entry
Emergency services	911 or 9911
Local	9 + 7 digits
Local BR2	9 + PSTN access code (0) + 10 digits
Long-distance (HQ and BR1 only)	9 + 1 + 10 digits
International (HQ and BR1 only)	9 + 011 + country code + variable number of digits

Location	Phone	Line/SD	Extension
HQ	1	Line 1 Executive	2001
	2	Line 2 Admin	2002
BR1	1	Line 1 Manager	3001
	2	Line 2 Admin	3005
BR2	1	Line 1 Engineer	4001
	2	Line 1 Admin	4002
		Line 2 Admin	4006
		Line 4 Lobby	4005

Task 1: Configure HQ

Big Rock Industries (BRI) is a producer of calcium carbonate products. It currently has two locations in the United States and a new quarry and processing facility in the United Kingdom. The United States facilities are designated HQ and BR1 and are supported by a centralized Cisco CallManager cluster at the HQ location. The new location in the United Kingdom has been designated BR2. All three locations are connected over a Frame Relay network. The proposed network drawing shows the layout of the Cisco CallManager cluster, gateways, Frame Relay connections, and IP addressing. The numbering plan for each location is also enclosed in this drawing. The domain name is bigrockind.com.

The staff at BRI has stated that it needs a number of services for its solution. It needs to support emergency services at all locations. It also needs to support a scalable and redundant E.164 address resolution.

Note The steps for this lab activity may not be linear.

Activity Procedure

Complete these steps:

- Step 1** HQ has been defined in Cisco CallManager. Verify that HQ phones can call emergency services and local numbers.
- Step 2** Configure the HQ router as a gatekeeper. Add a gatekeeper-controlled trunk to Cisco CallManager. Add the trunk to the existing BR2 route-list as the preferred route. Call the zone HQ. PSTN calls to BR2 need to be resolved by the gatekeeper.

Activity Verification

You have completed this task when you attain these results:

- You can make calls to emergency services and local numbers to verify that calls can be placed correctly.
- You can verify that the gatekeeper-controlled trunk is recognized by Cisco CallManager.
- You can place calls to both BR2 extensions to validate that the gatekeeper is resolving the addresses correctly between zones.

Task 2: Configure BR1

The BR1 location has a number of services that need to be supported. Because this is a location that is remote to HQ, you will need to consider how an IP WAN failure or loss of connectivity to the Cisco CallManager cluster will impact the users and thus to create a dial plan to support this function. Presently, the receptionist at HQ screens all the calls for BR1. The question is, how can this service be supported at BR1 without a dedicated receptionist? BRI is also concerned that calls from one location to another may be impacted by heavy call volume. Prepare the solution to keep call quality from being impacted by heavy volume but not by rejecting a call. If the Cisco CallManager or IP WAN becomes unavailable, ensure that users can dial only the same locations that they can when Cisco CallManager is functional.

Activity Procedure

Complete these steps:

- Step 1** Configure BR1 as an H.323 gateway. BR1 has already been defined in Cisco CallManager.

Controller Configuration

Step 3 Switch type	Step 4 basic-ni
Step 5 Framing	Step 6 ESF
Step 7 Line code	Step 8 B8ZS

- Step 2** BR1 has a PRI to the PSTN that supports six simultaneous calls. Configure appropriate dial peers to allow BR1 Cisco IP Phones to call emergency services and to make local, long-distance, and international calls.
- Step 3** BR1 should utilize the Cisco CallManager subscriber (10.1.5.3) for incoming PSTN calls. Calls should be sent to the Cisco CallManager publisher (10.1.5.2) if the subscriber is not available.
- Step 4** The PSTN sends the full E.164 number. Use appropriate digit manipulation to route incoming calls to the appropriate IP Phone.
- Step 5** Configure the gateway to allow calls to the PSTN for 911, seven-digit local numbers, 1+10 digits for long-distance calls, and 011+variable numbers for international calls.
- Step 6** BR1 should support local transcoding.
- Step 7** Configure BR1 for SRST support. Maintain the same CoS for IP Phones as in the lab activity “Implementing a Dial Plan and COR.” Maintain four-digit dialing to HQ and BR2 in SRST mode.

Class of Restriction

User Group	Dialing Capabilities
Executives	Unrestricted dialing
Sales administrators	Internal, local, and long-distance calls
Engineers	Unrestricted dialing
Administrators	Internal and local calls
Lobby and breakroom	Internal calls

- Step 8** Incoming calls to 3000 should be handled by an Auto Attendant while in SRST mode.
- Step 9** Configure COR in such a manner so that all the phones at BR1 cannot call extension 4002 at BR2.
- Step 10** MoH should be available in SRST mode.

Activity Verification

You have completed this task when you attain these results:

- Make calls to emergency services and local numbers to verify that calls can be placed correctly.
- Verify that redundant Cisco CallManagers are supported.
- Make a call from another location across the PSTN to ensure that calls are handled correctly.
- Verify that SRST becomes active and calls can be placed to all other locations and be received from all other locations.
- Verify MoH operation by placing a call to another location and then placing it on hold.
- Verify that only one call can cross the IP WAN and all subsequent calls are routed across the PSTN.
- Under SRST operation, verify that the Auto Attendant pilot point is functioning correctly.

Task 3: Configure BR2

BR2 has some specific requirements. The engineers are located in an office in the quarry. Their phones need to call other extensions on site and emergency services only. Because this branch is connected to the U.S. headquarters via a Frame Relay IP WAN, the BRI telephony staff is concerned that bandwidth will be quickly consumed by conferencing sessions. Consider how this problem can be resolved and deploy a solution. This location has an Auto Attendant to keep personnel costs down. Any calls that are not explicitly resolved should be routed to the administrator.

Please refer to the Job Aids tables for specific numbers.

Activity Procedure

Complete these steps:

- Step 1** Configure an E1 for four DS-0S's for R2-Compelled and DTMF at BR2 to provide four-digit dialing to HQ and BR1. Configure appropriate dial peers to support calling emergency services and local calling.
- Step 2** Implement the calling privileges from the table where applicable, except for these differences:
- Engineering phones should be able to call internal and emergency numbers only.
 - Administrators should have full calling privileges.

Class of Restriction

User Group	Dialing Capabilities
Executives	Unrestricted dialing
Sales administrators	Internal, local, and long-distance calls
Engineers	Unrestricted dialing
Administrators	Internal and local calls
Lobby and breakroom	Internal calls

- Step 3** BR2 should support local transcoding for CME.
- Step 4** Provide MoH.
- Step 5** Configure BR2GK as a gatekeeper. The local zone is BR2. Resolve calls to HQ via the gatekeeper.

Activity Verification

You have completed this task when you attain these results:

- You can use four-digit dialing to reach all extensions at HQ and BR1.
- The engineering phone is able to dial only emergency and local numbers.
- When calls are placed on hold, MoH plays.
- The gatekeeper resolves E.164 addresses.

Lab 6-1 Answer Key: Comprehensive Lab

When you complete this activity, your lab configuration will be similar to the results here, with differences that are specific to your device or workgroup:

HQ Solution Configuration

```
Pod7-HQ#sho run
Building configuration...

Current configuration : 2420 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Pod7-HQ
!
boot-start-marker
boot system flash:c2600-jsx-mz.123-11.T.bin
boot-end-marker
!
enable password cisco
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no aaa new-model
ip subnet-zero
!
!
ip cef
no ip domain lookup
ip dhcp excluded-address 10.1.10.1 10.1.10.100
ip dhcp excluded-address 10.1.110.1 10.1.110.50
!
ip dhcp pool Data
network 10.1.10.0 255.255.255.0
default-router 10.1.10.1
!
ip dhcp pool VOICE
network 10.1.110.0 255.255.255.0
option 150 ip 10.1.110.1
default-router 10.1.110.1
!
ip multicast-routing
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.5
description HQ Server VLAN
encapsulation dot1Q 5
ip address 10.1.5.1 255.255.255.0
!
interface FastEthernet0/0.10
description HQ Data VLAN
encapsulation dot1Q 10
ip address 10.1.10.1 255.255.255.0
!
interface FastEthernet0/0.110
encapsulation dot1Q 110
ip address 10.1.110.1 255.255.255.0
```

```

!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface ATM1/0
  no ip address
  no atm ilmi-keepalive
  ima-group 0
  no scrambling-payload
  cablelength short 133
!
interface ATM1/1
  no ip address
  shutdown
  no atm ilmi-keepalive
  no scrambling-payload
!
interface ATM1/2
  no ip address
  shutdown
  no atm ilmi-keepalive
  no scrambling-payload
!
interface ATM1/3
  no ip address
  shutdown
  no atm ilmi-keepalive
  no scrambling-payload
!
interface ATM1/IMA0
  no ip address
  no atm ilmi-keepalive
!
interface ATM1/IMA0.701 point-to-point
  ip address 10.12.1.1 255.255.255.0
  ip pim dense-mode
  pvc br1pvc 7/1
    broadcast
    encapsulation aal5snap
!
interface ATM1/IMA0.702 point-to-point
  ip address 10.13.1.1 255.255.255.0
  ip pim dense-mode
  pvc br2pvc 7/2
    broadcast
    encapsulation aal5snap
!
router eigrp 10
  network 10.0.0.0
  no auto-summary
!
ip http server
ip classless
!
ip pim bidir-enable
!
control-plane
!
dial-peer cor custom
!
gatekeeper
  zone local HQ bigrockind.com 10.1.110.1
  zone remote BR2 bigrockind.com 10.3.30.30 1719
  zone prefix HQ 2...
  zone prefix HQ 3...

```

```

zone prefix BR2 4...
gw-type-prefix 1#* default-technology
no shutdown
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password cisco
login
!
end

```

BR1 Solution Configuration

```

Pod7-BR1#sho run
Building configuration...

Current configuration : 6214 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Pod7-BR1
!
boot-start-marker
boot system flash c3725-ipvoice-mz.123-11.T.bin
boot-end-marker
!
enable password cisco
!
no network-clock-participate slot 1
voice-card 1
dspfarm
dsp services dspfarm
!
no aaa new-model
ip subnet-zero
ip cef
!
ip dhcp excluded-address 10.2.20.1 10.2.20.50
ip dhcp excluded-address 10.2.120.1 10.2.120.50
!
ip dhcp pool DATA
network 10.2.20.0 255.255.255.0
default-router 10.2.20.1
!
ip dhcp pool VOICE
network 10.2.120.0 255.255.255.0
option 150 ip 10.1.5.2
default-router 10.2.120.1
!
no ip domain lookup
ip multicast-routing
no ftp-server write-enable
isdn switch-type primary-ni
!
voice translation-rule 1
rule 1 /^.*\(\...\)/ /\1/
!
voice translation-rule 2
rule 1 /^307\(\3...\)$/ /\1/
!
voice translation-profile keep4
translate called 1
!

```

```

voice translation-profile localin
  translate called 2
!
controller T1 1/0
  framing esf
  linecode b8zs
  pri-group timeslots 1-6,24
!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/0
  no ip address
  encapsulation frame-relay IETF
  no fair-queue
  frame-relay lmi-type ansi
!
interface Serial0/0.701 point-to-point
  ip address 10.12.1.2 255.255.255.0
  frame-relay interface-dlci 701
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial1/0:23
  no ip address
  isdn switch-type primary-ni
  isdn incoming-voice voice
  no cdp enable
!
interface FastEthernet2/0
  no ip address
  shutdown
!
interface FastEthernet2/1
  description Branch-1 IP Phone 1
  switchport trunk native vlan 20
  switchport mode trunk
  switchport voice vlan 120
  no ip address
!
interface FastEthernet2/2
  description Branch-1 IP Phone 2
  switchport trunk native vlan 20
  switchport mode trunk
  switchport voice vlan 120
  no ip address
!
interface FastEthernet2/3
  description Branch-1 IP ATA-188
  switchport trunk native vlan 20
  switchport mode trunk
  no ip address
!
interface FastEthernet2/4
  no ip address
  shutdown
!
interface FastEthernet2/5
  no ip address
  shutdown
!

```

```
interface FastEthernet2/6
no ip address
shutdown
!
interface FastEthernet2/7
no ip address
shutdown
!
interface FastEthernet2/8
no ip address
shutdown
!
interface FastEthernet2/9
no ip address
shutdown
!
interface FastEthernet2/10
no ip address
shutdown
!
interface FastEthernet2/11
no ip address
shutdown
!
interface FastEthernet2/12
no ip address
shutdown
!
interface FastEthernet2/13
no ip address
shutdown
!
interface FastEthernet2/14
no ip address
shutdown
!
interface FastEthernet2/15
no ip address
shutdown
!
interface FastEthernet2/16
no ip address
shutdown
!
interface FastEthernet2/17
no ip address
shutdown
!
interface FastEthernet2/18
no ip address
shutdown
!
interface FastEthernet2/19
no ip address
shutdown
!
interface FastEthernet2/20
no ip address
shutdown
!
interface FastEthernet2/21
no ip address
shutdown
!
interface FastEthernet2/22
no ip address
shutdown
!
```

```

interface FastEthernet2/23
  no ip address
  shutdown
!
interface FastEthernet2/24
  no ip address
  shutdown
!
interface FastEthernet2/25
  no ip address
  shutdown
!
interface FastEthernet2/26
  no ip address
  shutdown
!
interface FastEthernet2/27
  no ip address
  shutdown
!
interface FastEthernet2/28
  no ip address
  shutdown
!
interface FastEthernet2/29
  no ip address
  shutdown
!
interface FastEthernet2/30
  no ip address
  shutdown
!
interface FastEthernet2/31
  no ip address
  shutdown
!
interface FastEthernet2/32
  no ip address
  shutdown
!
interface FastEthernet2/33
  no ip address
  shutdown
!
interface FastEthernet2/34
  no ip address
  shutdown
!
interface FastEthernet2/35
  no ip address
  shutdown
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan20
  description Branch-1 Data VLAN
  ip address 10.2.20.1 255.255.255.0
!
interface Vlan120
  description Branch-1 VOICE VLAN
  ip address 10.2.120.1 255.255.255.0
  h323-gateway voip interface
  h323-gateway voip bind srcaddr 10.2.120.1
!
router eigrp 10
  network 10.0.0.0

```



```

no auto-summary
!
ip classless
!
ip http server
!
control-plane
!
call application voice AA flash:srst_CISCO.2.0.0.0.tcl
call application voice AA aa-pilot 3000
call application voice AA language 1 en
call application voice AA set-location en 0 flash://
!
voice-port 1/0:23
!
sccp local Vlan120
sccp
sccp ccm 10.1.5.3 priority 1
sccp ccm 10.1.5.2 priority 2
!
dspfarm transcoder maximum sessions 2
dspfarm
!
dial-peer cor custom
  name rest
  name intl
!
dial-peer cor list other-call
  member rest
!
dial-peer cor list intl-call
  member rest
  member intl
!
!
dial-peer voice 911 pots
  corlist outgoing other-call
  destination-pattern 911
  no digit-strip
  port 1/0:23
!
dial-peer voice 9911 pots
  corlist outgoing other-call
  destination-pattern 9911
  port 1/0:23
  prefix 911
!
dial-peer voice 91 pots
  corlist outgoing other-call
  destination-pattern 91[2-9]..[2-9].....
  port 1/0:23
  prefix 1
!
dial-peer voice 9011 pots
  corlist outgoing intl-call
  destination-pattern 9011T
  port 1/0:23
  prefix 011
!
dial-peer voice 97 pots
  corlist outgoing other-call
  destination-pattern 9[2-9].....
  port 1/0:23
!
dial-peer voice 1 pots
  translation-profile incoming keep4
  application aa
  incoming called-number .

```

```

direct-inward-dial
port 1/0:23
!
dial-peer voice 2 pots
corlist outgoing other-call
destination-pattern 2...
port 1/0:23
prefix 12072072
!
dial-peer voice 4 pots
corlist outgoing intl-call
destination-pattern 4...
port 1/0:23
prefix 011440788074
!
dial-peer voice 3 voip
destination-pattern 3...
session target ipv4:10.1.5.3
dtmf-relay h245-alphanumeric
no vad
!
dial-peer voice 31 voip
preference 1
destination-pattern 3...
session target ipv4:10.1.5.2
dtmf-relay h245-alphanumeric
no vad
!
call-manager-fallback
max-conferences 8
ip source-address 10.2.120.1 port 2000
max-ephones 6
max-dn 12
dialplan-pattern 1 3073073... extension-length 4
moh music-on-hold.au
cor incoming other-call default
cor incoming intl-call 1 3001
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password cisco
login
!
end

```

BR2 Solution Configuration

```

Pod7-BR2#sho run
Building configuration...

Current configuration : 4289 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Pod7-BR2
!
boot-start-marker
boot system flash:c3725-ipvoice-mz.123-11.T.bin
boot-end-marker
!
enable password cisco
!
no network-clock-participate slot 1

```

```

no network-clock-participate slot 2
voice-card 1
  dspfarm
  dsp services dspfarm
!
voice-card 2
  no dspfarm
!
no aaa new-model
ip subnet-zero
ip cef
!
ip dhcp excluded-address 10.3.30.1 10.3.30.50
ip dhcp excluded-address 10.3.130.1 10.3.130.50
!
ip dhcp pool Data
  network 10.3.30.0 255.255.255.0
  default-router 10.3.30.1
!
ip dhcp pool VOICE
  network 10.3.130.0 255.255.255.0
  default-router 10.3.130.1
  option 150 ip 10.3.130.1
!
no ip domain lookup
ip multicast-routing
no ftp-server write-enable
!
no voice call carrier capacity active
!
controller E1 1/0
  ds0-group 0 timeslots 1-4 type r2-digital dtmf dnis
!
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface FastEthernet0/0.30
  description Branch-2 Data VLAN
  encapsulation dot1Q 30
  ip address 10.3.30.1 255.255.255.0
!
interface FastEthernet0/0.130
  description Branch-2 VOICE VLAN
  encapsulation dot1Q 130
  ip address 10.3.130.1 255.255.255.0
  h323-gateway voip interface
  h323-gateway voip id BR2 ipaddr 10.3.30.30 1719
  h323-gateway voip h323-id BR2@bigrockind.com
  h323-gateway voip tech-prefix 1#
  h323-gateway voip bind srcaddr 10.3.130.1
!
interface Serial0/0
  no ip address
  encapsulation frame-relay IETF
  no fair-queue
  frame-relay lmi-type ansi
!
interface Serial0/0.702 point-to-point
  ip address 10.13.1.2 255.255.255.0
  frame-relay interface-dlci 702
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto

```

```

!
router eigrp 10
  network 10.0.0.0
  no auto-summary
!
ip classless
!
ip http server
!
control-plane
!
call application voice autoatt flash:its-CISCO.2.0.1.0.tcl
call application voice autoatt operator 4002
call application voice autoatt aa-pilot 4000
call application voice autoatt language 0 en
call application voice autoatt set-location en 0 flash:\\
!
voice-port 1/0:0
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/0/2
!
voice-port 2/0/3
!
sccp local FastEthernet0/0.30
sccp
sccp ccm 10.1.5.3 priority 1
sccp ccm 10.1.5.2 priority 2
!
dspfarm transcoder maximum sessions 2
dspfarm
!
dial-peer cor custom
  name internal
  name 911
  name other
!
dial-peer cor list Engineer
  member internal
  member 911
!
dial-peer cor list unrestricted
  member internal
  member 911
  member other
!
dial-peer cor list 911-call
  member 911
!
dial-peer cor list other-call
  member other
!
dial-peer cor list internal-call
  member internal
!
!
dial-peer voice 2000 voip
  corlist outgoing internal-call
  destination-pattern 2...
  session target ras
  dtmf-relay h245-alphanumeric
!
dial-peer voice 3000 voip
  corlist outgoing internal-call
  destination-pattern 3...

```

```

session target ras
dtmf-relay h245-alphanumeric
!
dial-peer voice 911 pots
corlist outgoing 911-call
destination-pattern 911
no digit-strip
port 1/0:0
!
dial-peer voice 9911 pots
corlist outgoing 911-call
destination-pattern 9911
port 1/0:0
prefix 911
!
dial-peer voice 97 pots
corlist outgoing other-call
destination-pattern 900788074...
port 1/0:0
prefix 00788074
!
dial-peer voice 1 pots
application autoatt
incoming called-number .
direct-inward-dial
port 1/0:0
!
gateway
timer receive-rtcp 1200
!
telephony-service
max-ephones 12
max-dn 12
ip source-address 10.3.130.1 port 2000
sdspfarm units 1
sdspfarm transcode sessions 6
sdspfarm tag 1 MTP000dbca0fdb0
create cnf-files version-stamp Jan 01 2002 00:00:00
dialplan-pattern 1 4400788074... extension-length 4
max-conferences 8
moh music-on-hold.au
!
ephone-dn 1
number 4001
label BR2 Engineer 4001
cor incoming Engineer
!
ephone-dn 2
number 4002
label BR2 Admin 4002
cor incoming unrestricted
!
ephone-dn 3
number 4006
label BR2 Admin 4006
cor incoming unrestricted
!
ephone-dn 5
number 4005
label Lobby 4005
cor incoming Engineer
!
ephone 1
mac-address 000D.BC04.9BCD
button 1:1
!
ephone 2
mac-address 000D.2858.8043

```

```
button 1:2 2:3 4:5
!  
line con 0  
  exec-timeout 0 0  
line aux 0  
line vty 0 4  
  password cisco  
  login  
!  
end
```