

CVOICE

Cisco Voice over IP

Volumes 1 & 2

Version 5.0

Student Guide

QACS Production Services: 02.20.06

Copyright © 2006, 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 © 2006 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
Course Goal and Objectives	1
Course Outline	2
Cisco Certifications	3
Learner Skills and Knowledge	4
Learner Responsibilities	5
General Administration	6
Course Flow Diagram	7
Icons and Symbols	8
Learner Introductions	9
<i>Introduction to VoIP</i>	1-1
Overview	1-1
Module Objectives	1-1
Module Outline	1-2
<i>Introducing VoIP Network Technologies</i>	1-3
Overview	1-3
Relevance	1-3
Objectives	1-4
Learner Skills and Knowledge	1-4
Outline	1-5
Business CASE for VoIP	1-6
VoIP Functions	1-8
Components of a VoIP Network	1-10
VoIP Signaling Protocols	1-11
VoIP Service Considerations	1-14
RTP and RTCP	1-16
Example: RTP Application	1-17
Example: RTCP Application	1-18
Summary	1-19
References	1-20
Lesson Self-Check	1-21
Lesson Self-Check Answer Key	1-24
<i>Introducing VoIP Network Architectures</i>	1-25
Overview	1-25
Relevance	1-25
Objectives	1-25
Learner Skills and Knowledge	1-26
Outline	1-26
Centralized Network Architectures	1-27
Example: Centralized Network Architectures	1-28
Distributed Network Architectures Using H.323	1-29
Distributed Network Architectures Using SIP	1-31
Comparing Network Architectures	1-33
Example: Comparing Centralized and Distributed Call Control Models	1-34
Example: Simple Multisite IP Telephony Network	1-35
Interconnecting VoIP Protocols	1-37
Understanding Gateways	1-39
Example: Analog and Digital Gateways	1-39
Guidelines for Selecting the Correct Gateway	1-40
Example: Selecting a Gateway	1-41
Enterprise Central and Remote Site Gateway Interconnection Requirements	1-42
Example: Gateway Interconnect Considerations	1-43
Service Provider Gateway Interconnection Requirements	1-45

Example: Service Provider Requirements	1-46
Practice Item: Network Architecture	1-46
Practice Item Answer Key	1-48
Summary	1-49
References	1-50
Lesson Self-Check	1-51
Lesson Self-Check Answer Key	1-55
Building Scalable Dial Plans	1-57
Overview	1-57
Relevance	1-57
Objectives	1-57
Learner Skills and Knowledge	1-58
Outline	1-58
Numbering and Dial Plans	1-59
Example 1: Span Engineering Numbering Plan	1-61
Example 2: Span Engineering Dial Plan	1-62
Example: Span Engineering Hierarchical Numbering Plan	1-64
Internal Numbering and Public Numbering Plan Integration	1-65
Example: Span Engineering Integration of Internal and Public Numbering Plans	1-67
Scalable Dial Plans	1-68
Example: Dial Plan Implementations	1-68
Practice Item 1: Span Engineering Dial Plan Worksheet	1-70
Practice Item 1 Answer Key	1-71
Scalable Dial Plan Attributes	1-72
Example: Span Engineering Dial Plan Attributes	1-73
Enhancing and Extending an Existing Numbering Plan to Accommodate VoIP	1-74
Example: Number Normalization	1-74
Example: Technology Prefixes Applied	1-75
Accounting for Caller Mobility for 911 Services	1-77
Example: 911 Call Processing in a Nonmobile Environment	1-79
Example: 911 Call Processing in a Mobile Environment	1-80
Practice Item 2: Numbering Plan for Span Engineering	1-81
Chicago Airport Location	1-81
London Location	1-81
Practice Item 2 Answer Key	1-82
Summary	1-83
References	1-84
Lesson Self-Check	1-85
Lesson Self-Check Answer Key	1-88
Calculating Bandwidth Requirements	1-89
Overview	1-89
Relevance	1-89
Objectives	1-89
Learner Skills and Knowledge	1-90
Outline	1-90
Codec Bandwidths	1-91
Impact of Voice Samples and Packet Size on Bandwidth	1-93
Example: Encapsulated Bytes Calculation	1-93
Data-Link Overhead	1-94
Security and Tunneling Overhead	1-95
Example: VPN Overhead	1-95
Calculating the Total Bandwidth for a VoIP Call	1-96
Example: Total Bandwidth Calculation for Span Engineering	1-97
Effects of VAD on Bandwidth	1-98
Example: Span Engineering VAD Bandwidth Savings	1-99
Practice Item: Span Engineering Voice Bandwidth Requirement	1-100
Practice Item Answer Key	1-101
Summary	1-102
References	1-102

Lesson Self-Check	1-103
Lesson Self-Check Answer Key	1-105
Allocating Bandwidth for Voice and Data Traffic	1-107
Overview	1-107
Relevance	1-107
Objectives	1-107
Learner Skills and Knowledge	1-108
Outline	1-108
Sources of Traffic Statistics	1-109
Example: Gathering Statistics	1-109
Network Objectives for Voice and Data	1-111
Example: Grade of Service Value	1-111
Meeting the Current Network Objective	1-112
Example: Network Demand	1-113
Traffic Theory	1-114
Busy Hour	1-116
Erlangs	1-117
Example: Erlang Calculation	1-117
Traffic Probability Assumptions	1-118
Example: Traffic Arrival Assumption	1-119
Traffic Calculations	1-120
Example: Traffic Calculations	1-121
Call Density Matrix	1-122
Example: Call Density Matrix	1-122
Bandwidth Calculations	1-123
Determining IP Bandwidth	1-123
Practice Item: Bandwidth Calculation	1-126
Practice Item Answer Key	1-128
Summary	1-129
Lesson Self-Check	1-130
Lesson Self-Check Answer Key	1-134
Considering Security Implications of VoIP Networks	1-137
Overview	1-137
Relevance	1-137
Objectives	1-137
Learner Skills and Knowledge	1-138
Outline	1-138
Security Policies for VoIP Networks	1-139
Example: Networkwide Security	1-140
Threats to VoIP	1-141
Secure LAN Design	1-143
Communicating Through a Firewall	1-144
Example: Stateful Firewall	1-145
Delivering VoIP over a VPN	1-146
International Issues	1-147
Bandwidth Overhead Associated with a VPN	1-148
Example: VPN Bandwidth	1-149
Practice Item: Span Engineering VoIP Network Security Components	1-150
Practice Item Answer Key	1-152
Summary	1-153
References	1-153
Lesson Self-Check	1-154
Lesson Self-Check Answer Key	1-156
Configuring Voice Networks	2-1
Overview	2-1
Module Objectives	2-1
Module Outline	2-2

Configuring Router Voice Ports	2-3
Overview	2-3
Relevance	2-3
Objectives	2-3
Learner Skills and Knowledge	2-4
Outline	2-4
Voice Port Applications	2-5
Example: Voice Port Applications	2-12
FXS Ports	2-13
Example: When to Configure FXS Ports	2-13
Configuration Parameters	2-14
Example: FXS Port Configuration	2-15
FXO Ports	2-16
Configuration Parameters	2-16
Example: FXO Port Configuration	2-17
E&M Ports	2-18
Configuration Parameters	2-18
Example: E&M Port Configuration	2-19
Timers and Timing	2-20
Configuration Parameters	2-20
Example: Timers Configuration	2-21
Digital Voice Ports	2-22
Configuration Parameters	2-22
Example: T1 Configuration	2-24
ISDN	2-25
Configuration Parameters	2-25
Example: ISDN QSIG Configuration	2-26
CCS Options	2-27
T-CCS Configuration Process	2-28
Monitoring and Troubleshooting	2-29
Summary	2-33
References	2-34
Next Steps	2-34
Lesson Self-Check	2-35
Lesson Self-Check Answer Key	2-38
Adjusting Voice Interface Settings	2-41
Overview	2-41
Relevance	2-41
Objectives	2-41
Learner Skills and Knowledge	2-41
Outline	2-42
Factors Affecting Voice Quality	2-43
Setting Input and Output Power Levels	2-45
Baselining Input and Output Power Levels	2-45
Example: Decibel Levels	2-46
Voice Quality Tuning	2-47
Configuration Parameters	2-48
Example: Voice Port Tuning	2-49
Echo Cancellation Commands	2-50
Example: Echo Suppression Applied	2-51
Summary	2-53
References	2-53
Next Steps	2-53
Lesson Self-Check	2-54
Lesson Self-Check Answer Key	2-56

Configuring Dial Peers	2-57
Overview	2-57
Relevance	2-57
Objectives	2-57
Learner Skills and Knowledge	2-58
Outline	2-59
Dial Peers and Call Legs	2-60
Example: Call Legs Defined	2-60
End-to-End Calls	2-61
Types of Dial Peers	2-63
Example: Dial-Peer Configuration	2-65
Configuring POTS Dial Peers	2-66
Example: POTS Dial-Peer Configuration	2-67
Practice Item 1: POTS Dial-Peer Configuration	2-67
Configuring VoIP Dial Peers	2-69
Example: VoIP Dial-Peer Configuration	2-70
Practice Item 2: VoIP Dial-Peer Configuration	2-71
Configuring Destination-Pattern Options	2-72
Example: Matching Destination Patterns	2-74
Default Dial Peer	2-75
Example: Use of Default Dial Peer	2-75
Matching Inbound Dial Peers	2-77
Practice Item 3: Matching Inbound Dial Peers	2-79
Matching Outbound Dial Peers	2-80
Example: Matching Outbound Dial Peers	2-81
Configuring Hunt Groups	2-82
Example: Hunt-Group Application	2-85
Practice Item 4: Configuring Hunt Groups	2-86
Digit Collection and Consumption	2-87
Example: Digit Collection	2-88
Configuring Digit Manipulation	2-90
Example: Using Digit Manipulation Tools	2-92
Practice Item 5: Digit Manipulation	2-94
Summary	2-95
References	2-96
Next Steps	2-96
Lesson Self-Check	2-97
Lesson Self-Check Answer Key	2-103
Configuring Voice Port Network Connections	2-105
Overview	2-105
Relevance	2-105
Objectives	2-105
Learner Skills and Knowledge	2-106
Outline	2-107
Connection Types	2-108
Using the connection Command	2-110
Configuring PLAR Connections	2-112
Configuring PLAR OPX Connections	2-113
Configuring Trunk Connections	2-114
Configuring Tie-Line Connections	2-116
Summary	2-117
References	2-118
Next Steps	2-118
Lesson Self-Check	2-119
Lesson Self-Check Answer Key	2-121

Volume 2

<i>VoIP Signaling and Call Control</i>	3-1
Overview	3-1
Module Objectives	3-2
Module Outline	3-2
<i>Introducing Signaling and Call Control</i>	3-3
Overview	3-3
Relevance	3-3
Objectives	3-3
Learner Skills and Knowledge	3-3
Outline	3-4
VoIP Signaling	3-5
Call Control Models	3-7
Translation Between Signaling and Call Control Models	3-8
Example: Call Control Translation	3-9
Call Setup	3-10
Call Administration and Accounting	3-12
Call Status and CDRs	3-13
Address Management	3-14
Example: Address Registration	3-15
Admission Control	3-16
Summary	3-17
References	3-18
Lesson Self-Check	3-19
Lesson Self-Check Answer Key	3-22
<i>Introducing H.323</i>	3-25
Overview	3-25
Relevance	3-25
Objectives	3-25
Learner Skills and Knowledge	3-26
Outline	3-26
H.323 and IP	3-27
Example: H.323 Adapted to IP	3-29
Functional Components of H.323	3-30
H.323 Gateways	3-31
IP-to-IP Gateways	3-32
H.323 Gatekeepers	3-33
Multipoint Conferences	3-34
H.323 Call Establishment and Maintenance	3-35
RAS Messages	3-36
Call Flows Without a Gatekeeper	3-38
H.323 Fast Connect Call Setup	3-39
Call Flows with a Gatekeeper	3-40
Call Setup with a Gatekeeper	3-41
Gatekeeper-Routed Call Signaling	3-42
Call Flows with Multiple Gatekeepers	3-43
Call Setup with Multiple Gatekeepers	3-44
Multipoint Conferences	3-45
Summary	3-47
References	3-48
Lesson Self-Check	3-49
Lesson Self-Check Answer Key	3-52

Deploying and Configuring H.323	3-53
Overview	3-53
Relevance	3-53
Objectives	3-53
Learner Skills and Knowledge	3-53
Outline	3-54
Robust Design	3-55
H.323 Proxy Server	3-57
Example: H.323 Proxy	3-58
Cisco Implementation of H.323	3-59
Configuring H.323 Gateways	3-60
Configuring H.323 Gatekeepers	3-63
Monitoring and Troubleshooting	3-65
Selected debug Commands	3-66
Summary	3-67
References	3-67
Next Steps	3-67
Lesson Self-Check	3-68
Lesson Self-Check Answer Key	3-70
Configuring SIP	3-71
Overview	3-71
Relevance	3-71
Objectives	3-71
Learner Skills and Knowledge	3-72
Outline	3-72
Session Initiation Protocol	3-73
Example: Cisco SIP Support	3-74
Components of SIP	3-76
Example: SIP Applications	3-77
SIP Messages	3-78
Status Codes	3-80
SIP Addressing	3-81
Example: SIP Addressing Variants	3-81
Call Setup Models	3-84
Robust Design	3-87
Example: SIP Survivability	3-87
Cisco Implementation of SIP	3-88
Configuring SIP on a Cisco Router	3-89
Example: Configuring a SIP User Agent	3-89
Example: SIP Dial Peers	3-90
Monitoring and Troubleshooting	3-91
Summary	3-93
References	3-94
Next Steps	3-94
Lesson Self-Check	3-95
Lesson Self-Check Answer Key	3-98
Configuring MGCP	3-99
Overview	3-99
Relevance	3-99
Objectives	3-99
Learner Skills and Knowledge	3-100
Outline	3-101
MGCP and Its Associated Standards	3-102
Basic MGCP Components	3-103
Example: Cisco MGCP Components	3-103
MGCP Endpoints	3-104
Example: Endpoint Identifiers	3-105
MGCP Gateways	3-106

MGCP Call Agents	3-108
Basic MGCP Concepts	3-109
MGCP Calls and Connections	3-110
MGCP Control Messages	3-112
Call Flows	3-114
Robust Design	3-116
Cisco Implementation of MGCP	3-118
Configuring MGCP	3-119
Example: MGCP Residential Gateway Configuration	3-120
Example: Configuring an MGCP Trunk Gateway	3-120
Monitoring and Troubleshooting	3-121
Summary	3-123
References	3-124
Next Steps	3-124
Lesson Self-Check	3-125
Lesson Self-Check Answer Key	3-129

Comparing Call Control Models **3-131**

Overview	3-131
Relevance	3-131
Objectives	3-131
Learner Skills and Knowledge	3-131
Outline	3-132
Feature Comparison Charts	3-133
Standards Bodies (ITU-T vs. IETF)	3-134
Architecture (Centralized vs. Distributed)	3-134
Current Version	3-135
Signaling Transport (TCP vs. UDP)	3-135
Multimedia Capability (Yes or No)	3-135
Call Control Encoding (ASN.1 vs. Text)	3-135
Supplementary Services (Endpoint vs. Call Control)	3-135
Strengths of H.323, SIP, and MGCP	3-136
H.323	3-136
Session Initiation Protocol	3-136
Media Gateway Control Protocol	3-137
Selecting Appropriate Call Control	3-138
MGCP Call Control Model	3-138
The H.323 Call Control Model	3-139
SIP Call Control Model	3-140
Summary	3-141
References	3-141
Lesson Self-Check	3-142
Lesson Self-Check Answer Key	3-144

Improving and Maintaining Voice Quality **4-1**

Overview	4-1
Module Objectives	4-1
Module Outline	4-2

Designing for Optimal Voice Quality **4-3**

Overview	4-3
Objectives	4-3
Outline	4-4
IP Networking Overview	4-5
Jitter	4-7
Example: Jitter in Voice Networks	4-7
Delay	4-8
Acceptable Delay	4-9
Example: Acceptable Delay	4-10
Packet Loss	4-11
Example: Packet Loss in Voice Networks	4-11

PESQ, MOS, and PSQM	4-12
Mean Opinion Score	4-12
Perceptual Speech Quality Measurement	4-13
Perceptual Evaluation of Speech Quality	4-13
Quality Measurement Comparison	4-14
Objectives of QoS	4-16
Example: QoS Objectives	4-16
Using QoS to Improve Voice Quality	4-18
Recognizing Common Design Faults	4-20
Example: Deploying QoS	4-21
Cisco AutoQoS Features	4-22
Example: Span Engineering Implementation of Cisco AutoQoS	4-24
Summary	4-26
References	4-27
Lesson Self-Check	4-28
Lesson Self-Check Answer Key	4-31

Implementing CAC **4-33**

Overview	4-33
Relevance	4-33
Objectives	4-33
Learner Skills and Knowledge	4-33
Outline	4-34
Effects of Oversubscribing Bandwidth	4-35
Example: Oversubscription	4-35
CAC Operation	4-36
Example: Call Control CAC	4-36
Resource Reservation Protocol	4-37
Example: RSVP	4-38
CAC Tools	4-39
H.323 CAC	4-40
Example: H.323 CAC Configuration	4-44
SIP CAC	4-45
Configuring SAA RTR Responder	4-45
Configuring PSTN Fallback	4-46
Configuring Resource Availability Check	4-47
Example: SIP CAC Configuration	4-50
MGCP CAC	4-51
Configuring SRC CAC	4-52
Configuring RSVP CAC	4-53
Configuring Cisco SAA CAC	4-53
Example: MGCP VoIP CAC on a Trunking Gateway	4-54
Cisco CallManager CAC	4-57
Summary	4-58
References	4-59
Lesson Self-Check	4-60
Lesson Self-Check Answer Key	4-63

Course Introduction

Overview

Cisco Voice over IP (CVOICE) v5.0 provides an explanation of converged voice and data networks and the challenges faced by the various network technologies. The course presents Cisco solutions and implementation considerations to address those challenges.

Course Goal and Objectives

This section describes the course goal and objectives.

Course Goal

“To provide an understanding of converged voice and data networks as well as the challenges faced by their various technologies”

Cisco Voice over IP (CVOICE) v5.0

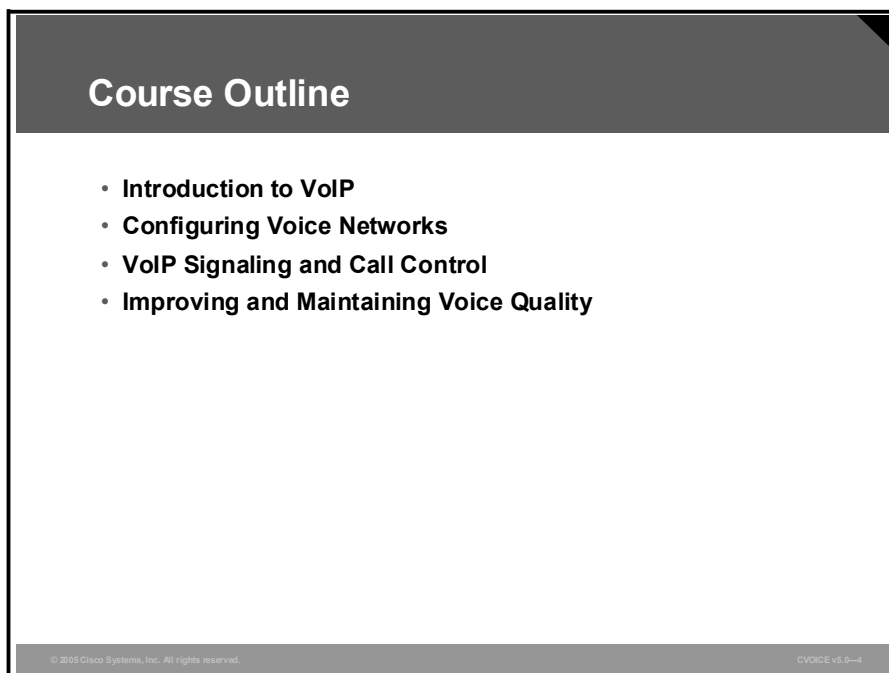
© 2005 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3

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

- Describe the architectures, components, and signaling protocols of VoIP and discuss traffic engineering and security requirements
- Configure voice interfaces on Cisco voice-enabled equipment for connection to traditional, nonpacketized telephony equipment; define and configure POTS and VoIP dial peers; configure voice ports for various connection types
- Compare centralized and decentralized call control and signaling protocols
- Describe specific voice quality issues and the QoS solutions used to solve them

Course Outline

The outline lists the modules included in this course.

A slide titled "Course Outline" with a dark grey header and footer. The main content area is white and contains a bulleted list of four modules. The footer contains copyright information and a version number.

Course Outline

- **Introduction to VoIP**
- **Configuring Voice Networks**
- **VoIP Signaling and Call Control**
- **Improving and Maintaining Voice Quality**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-4

Cisco Certifications

This topic lists the certification requirements of this course.

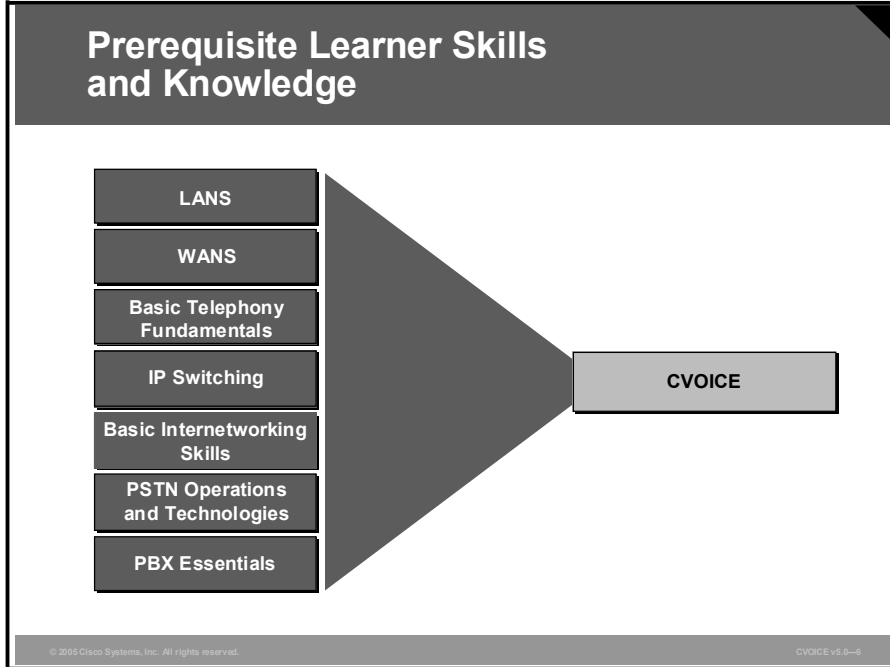


Cisco provides three levels of general career certifications for IT professionals with several different tracks to meet individual needs. Cisco also provides a variety of Cisco Qualified Specialist (CQS) certifications, which enable learners to demonstrate knowledge in specific technologies, solutions, or job roles. In contrast to general certifications, each CQS certification is focused on a designated area such as cable communications, voice, or security. All CQS certifications are customized to meet current market needs. They may also have special focused prerequisite requirements.

There are many paths to Cisco certification, but only one requirement—passing one or more exams demonstrating knowledge and skill. For details, go to <http://www.cisco.com/go/certifications>.

Learner Skills and Knowledge

This topic lists the course prerequisites.



To benefit fully from this course, you must have these prerequisite skills and knowledge:

- A working knowledge of LANs, WANs, and IP switching and routing
- Basic internetworking skills taught in the *Interconnecting Cisco Network Devices (ICND)* course, or its equivalent
- Knowledge of traditional public switched telephone network (PSTN) operations and voice fundamentals

Learner Responsibilities

This topic discusses the responsibilities of the learners.

Learner Responsibilities



- **Complete prerequisites**
- **Introduce yourself**
- **Ask questions**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-7

To take full advantage of the information that is presented in this course, you must have completed the prerequisite requirements.

In class, you are expected to participate in all lesson exercises and assessments.

In addition, you are encouraged to ask any questions that are relevant to the course materials.

If you have pertinent information or questions concerning future Cisco product releases and product features, please discuss these topics during breaks or after class. The instructor will answer your questions or direct you to an appropriate information source.

General Administration

This topic lists the administrative issues for the course.

General Administration

<p>Class-Related</p> <ul style="list-style-type: none">• Sign-in sheet• Course materials• Length and times• Attire	<p>Facilities-Related</p> <ul style="list-style-type: none">• Site emergency procedures• Rest rooms• Telephones/faxes• Break and lunchroom locations
--	--

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3

The instructor will discuss these administrative issues:

- Sign-in process
- Starting and anticipated ending times of each class day
- Class breaks and lunch facilities
- Appropriate attire during class
- Materials that you can expect to receive during class
- What to do in the event of an emergency
- Location of the rest rooms
- How to send and receive telephone and fax messages

Course Flow Diagram

This topic covers the suggested flow of the course materials.

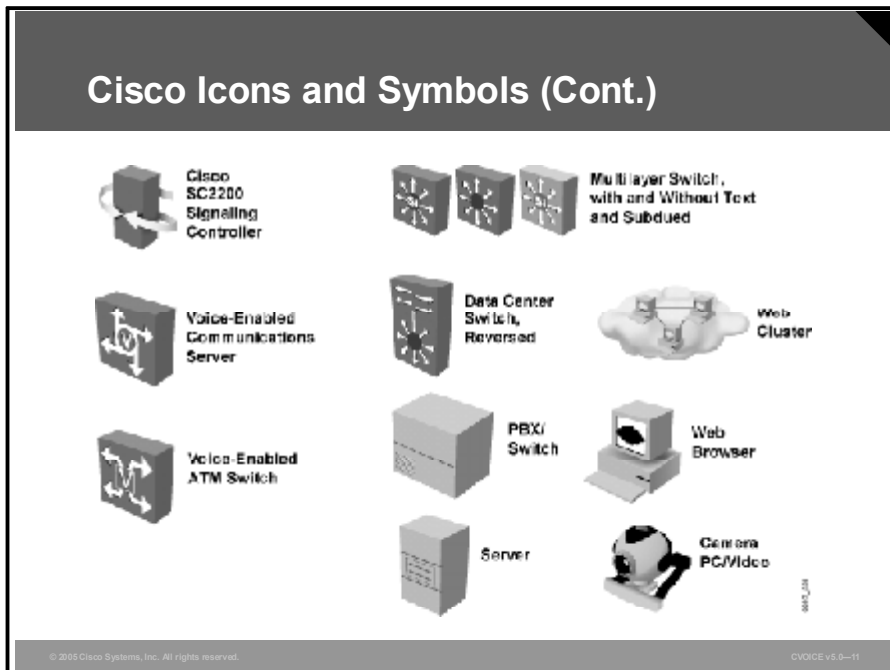
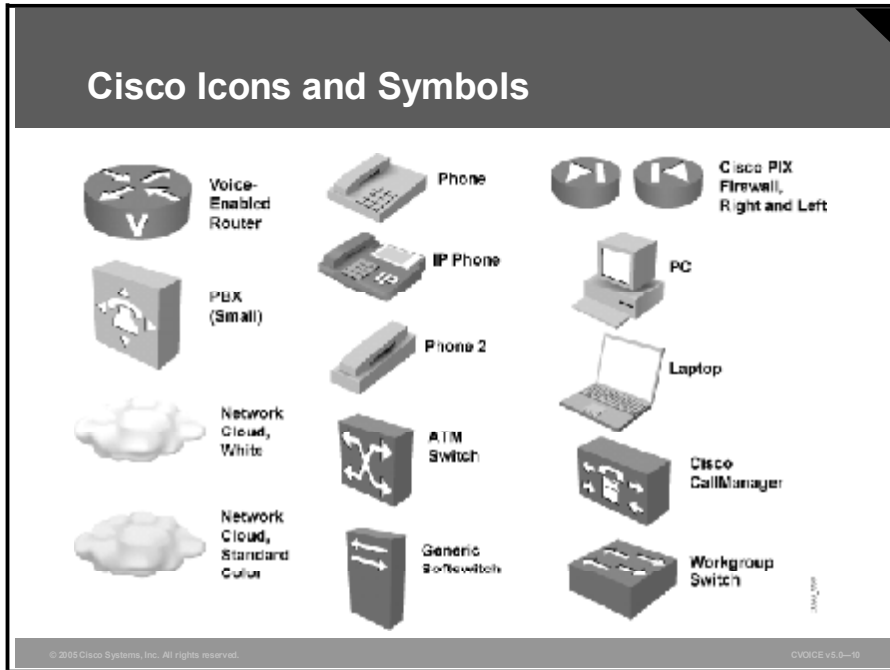
Course Flow Diagram					
		Day 1	Day 2	Day 3	Day 4
A M		Course Introduction	Configuring Voice Networks	Configuring Voice Networks (Cont.)	VoIP Signaling and Call Control (Cont.)
		Introduction to VoIP		VoIP Signaling and Call Control	Improving and Maintaining Voice Quality
Lunch					
P M		Introducing Voice over IP (Cont.)	Configuring Voice Networks (Cont.)	VoIP Signaling and Call Control (Cont.)	Improving and Maintaining Voice Quality (Cont.)

© 2005 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-9

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 laboratory exercises. The exact timing of the subject materials and labs depends on the pace of your specific class.

Icons and Symbols

This topic shows the Cisco icons and symbols used in this course.




Learner Introductions

This is the point in the course where you introduce yourself.

Learner Introductions

- **Your name**
- **Your company**
- **Skills and knowledge**
- **Brief history**
- **Objective**



© 2006 Cisco Systems, Inc. All rights reserved. OVOICE V5.0-12

Prepare to share the following information:

- Your name
- Your company
- If you have most or all of the prerequisite skills
- A profile of your experience
- What you would like to learn from this course

Module 1

Introduction to VoIP

Overview

Voice over IP (VoIP) enables a voice-enabled router to carry voice traffic, such as telephone calls and faxes, over an IP network. This module introduces the fundamentals of VoIP, discussing components of a VoIP network, architecture types, and available voice-signaling protocols. Numbering plans, dial plans, and VoIP access to 911 emergency services are explained. The module discusses the role of gateways and their use in integrating VoIP with traditional voice technologies. Traffic engineering and bandwidth calculations are also discussed. In addition, this module explains the impact of security threats and the components required for a secure voice network.

Module Objectives

Upon completing this module, you will be able to describe the architectures, components, and signaling protocols of VoIP and discuss traffic engineering and security requirements.

Module Objectives

- Describe how key VoIP technologies overcome data network challenges to provide cost-efficient and feature-rich voice-enabled networks.
- Describe the key components of a VoIP network in centralized and distributed architectures.
- Develop scalable dial plans to meet both domestic and overseas requirements.
- List the bandwidth requirements for various codecs and data links and describe the methods to reduce bandwidth consumption.
- Allocate bandwidth for voice and data traffic.
- Describe the implications of implementing security measures in IP networks that will transport voice.

Module Outline

The outline lists the components of this module.

Module Outline

- **Introducing VoIP Network Technologies**
- **Introducing VoIP Network Architectures**
- **Building Scalable Dial Plans**
- **Calculating Bandwidth Requirements**
- **Allocating Bandwidth for Voice and Data Traffic**
- **Considering Security Implications of VoIP Networks**

© 2005 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1.3

Lesson 1

Introducing VoIP Network Technologies

Overview

This lesson investigates the business drivers for Voice over IP (VoIP) implementations, the components required in VoIP networks, currently available signaling protocols, and service issues and their recommended solutions.

Relevance

The increased efficiency of packet networks and the ability to statistically multiplex voice traffic with data packets allows companies to maximize their return on investment (ROI) in data network infrastructures. Decreased cost and an increase in the availability of differentiating services are two major reasons why companies are evaluating the implementation of VoIP.

As demand for voice services in the IP network expands, it is important to understand the components and functionality that must be present for a successful implementation. Several protocols and tools are available for carrying voice in a data network. In defining the VoIP protocol stack, you must understand at which layer these tools and protocols reside and how they interact with other layers. When voice is packaged into IP packets, additional headers are created to carry voice-specific information. These headers can create significant additional overhead in the IP network.

Understanding which protocols to use and knowing how to limit overhead is crucial in carrying voice efficiently across the network.

Objectives

Upon completing this lesson, you will be able to describe how key VoIP technologies overcome data network challenges to provide cost-efficient and feature-rich voice-enabled networks. This ability includes being able to meet these objectives:

- Describe the business advantages of VoIP networks
- Compare the signaling, database services, bearer control, and codec functions of VoIP and PSTN
- Describe the main components of a VoIP network, including IP-enabled PBX, end-user devices, gateways and gatekeepers, and the IP network
- Describe the common protocols used in VoIP networks, including H.323, MGCP, SIP, Megaco protocol (also known as H.248), RTP, and RTCP, in terms of their application in centralized and distributed VoIP architectures
- Match VoIP protocols to the seven layers of the OSI model
- Identify a solution for latency, jitter, bandwidth, packet loss, reliability, and security issues in IP networks
- Explain the benefits of RTP and RTCP in terms of enabling the destination device to reorder and retime voice packets

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- General knowledge of telephony technology
- General knowledge of networking terminology and IP network concepts
- General knowledge of the seven-layer OSI model
- General knowledge of header compression

Outline

The outline lists the topics included in this lesson.

Outline

- **Overview**
- **Business Case for VoIP**
- **VoIP Functions**
- **Components of a VoIP Network**
- **VoIP Signaling Protocols**
- **VoIP Protocols and the OSI Model**
- **VoIP Service Considerations**
- **RTP and RTCP**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v6.0-1-2

Business CASE for VoIP

This topic describes the business advantages that drive current implementations of VoIP.

Business Case for VoIP

- **Cost savings**
- **Flexibility**
- **Advanced features:**
 - **Advanced call routing**
 - **Unified messaging**
 - **Integrated information systems**
 - **Long-distance toll bypass**
 - **Encryption**
 - **Customer relationship**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-3

The business advantages that drive implementations of VoIP networks have changed over time. Starting with simple media convergence, these advantages have evolved to include the convergence of call-switching intelligence and the total user experience.

Originally, ROI calculations centered on toll-bypass and converged-network savings. Although these savings are still relevant today, advances in voice technologies allow organizations and service providers to differentiate their product offerings by providing advanced features.

Here are some of the VoIP business drivers:

- **Cost savings:** Traditional time-division multiplexing (TDM), which is used in the public switched telephone network (PSTN) environment, dedicates 64 kbps of bandwidth per voice channel. This approach results in bandwidth being wasted when there is no voice to transmit. VoIP shares bandwidth among multiple logical connections, which makes more efficient use of the bandwidth, thereby reducing bandwidth requirements. A substantial amount of equipment is needed to combine 64-kbps channels into high-speed links for transport across the network. Packet telephony statistically multiplexes voice traffic alongside data traffic. This consolidation results in substantial savings on capital equipment and operations costs.
- **Flexibility:** The sophisticated functionality of IP networks allows organizations to be flexible in the types of applications and services that they provide to their customers and users. Service providers can easily segment customers. This helps service providers to provide different applications, custom services, and rates depending on the traffic volume needs of the customer and other factors.

- **Advanced features:** Here are some examples of the advanced features provided by current VoIP applications.
 - **Advanced call routing:** When multiple paths exist to connect a call to its destination, some of these paths may be preferred over others based on cost, distance, quality, partner handoffs, traffic load, or various other considerations. Least-cost routing and time-of-day routing are two examples of advanced call routing that can be implemented to determine the best possible route for each call.
 - **Unified messaging:** Unified messaging improves communications and boosts productivity. It delivers this advantage by providing a single user interface to messages that have been delivered over a variety of mediums. For example, users can read their e-mail, hear their voice mail, and view fax messages by accessing a single inbox.
 - **Integrated information systems:** Organizations are using VoIP to affect business process transformation. Centralized call control, geographically dispersed virtual contact centers, and access to resources and self-help tools are examples of VoIP technology that have enabled organizations to draw from a broad range of resources to service customers.
 - **Long-distance toll bypass:** Long-distance toll bypass is an attractive solution for organizations that place a significant number of calls between sites that are charged long-distance fees. In this case, it may be more cost-effective to use VoIP to place those calls across the IP network. If the IP WAN becomes congested, the calls can overflow into the PSTN, ensuring that there is no degradation in voice quality.
 - **Encryption:** Security mechanisms in the IP network allow the administrator to ensure that IP conversations are secure. Encryption of sensitive signaling header fields and message bodies protects the packet in case of unauthorized packet interception.
 - **Customer relationship:** The ability to provide customer support through multiple mediums, such as telephone, chat, and e-mail, builds solid customer satisfaction and loyalty. A pervasive IP network allows organizations to provide contact center agents with consolidated and up-to-date customer records along with the related customer communication. Access to this information allows quick problem solving, which, in turn, builds strong customer relationships.

VoIP Functions

This topic describes the signaling, database services, bearer control (call connect and call disconnect), and coder-decoder (codec) functions of VoIP in terms of how they compare to similar functions of PSTN.

VoIP Functions

- **Signaling**
 - **SS7, H.323, SIP, MGCP, H.248**
- **Database services**
 - **Billing, caller ID, toll-free numbers**
- **Bearer control**
 - **Call connect**
 - **Call disconnect**
- **Codecs**
 - **G.711, G.729**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1.4

In the traditional PSTN telephony network, all the elements that are required to complete the call are transparent to the end user. Migration to VoIP requires an awareness of these required elements and a thorough understanding of the protocols and components that provide the same functionality in an IP network.

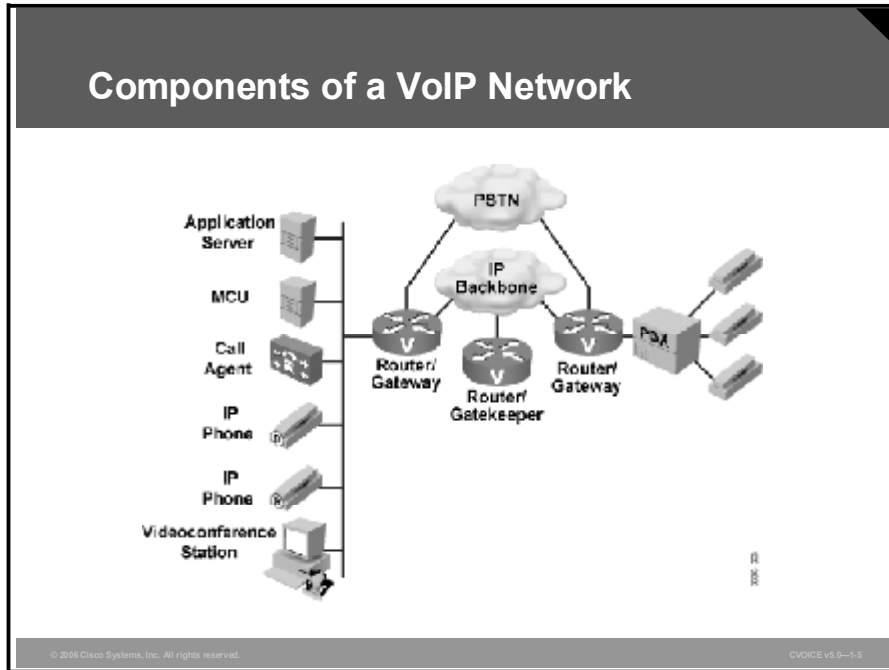
Required VoIP functionality includes these features:

- **Signaling:** Signaling is the ability to generate and exchange control information to establish, monitor, and release connections between two endpoints. Voice signaling requires the ability to provide supervisory, address, and alerting functionality between nodes. The PSTN network uses Signaling System 7 (SS7) to transport control messages in an out-of-band signaling network. VoIP presents several options for signaling, including H.323, session initiation protocol (SIP), H.248, and Media Gateway Control Protocol (MGCP). Some VoIP gateways are also capable of initiating SS7 signaling directly to the PSTN network. Signaling protocols are classified either as peer-to-peer or client/server architectures. SIP and H.323 are examples of peer-to-peer signaling protocols where the end devices or gateways contain the intelligence to initiate and terminate calls and interpret call control messages. H.248 and MGCP are examples of client/server protocols where the endpoints or gateways do not contain call control intelligence but send or receive event notifications to the server commonly referred to as the call agent. For example, when an MGCP gateway detects that a telephone has gone off hook, it does not know to automatically provide a dial tone. The gateway sends an event notification to the call agent, telling the agent that an off-hook condition has been detected. The call agent notifies the gateway to provide a dial tone.

- **Database services:** Access to services, such as toll-free numbers or caller ID, requires the ability to query a database to determine whether the call can be placed or the information made available. Database services include access to billing information, caller name delivery (CNAM), toll-free database services, and calling-card services. VoIP service providers can differentiate their services by providing access to numerous and unique database services. For example, to simplify fax access to mobile users, a provider may build a service that converts fax to e-mail. Another example would be to provide a call notification service that places outbound calls with prerecorded messages at specific times to notify users of such events as school closures, wakeup calls, or appointment reminders.
- **Bearer control:** Bearer channels are the channels that carry voice calls. Proper supervision of these channels requires that the appropriate call connect and call disconnect signaling be passed between end devices. Correct signaling ensures that the channel is allocated to the current voice call and that the channel is properly de-allocated when either side terminates the call. These connect and disconnect messages are carried in SS7 within the PSTN network, and these connect and disconnect message are carried in SIP, H.323, H.248, or MGCP within the IP network.
- **Codecs:** Codecs provide the coding and decoding translation between analog and digital facilities. Each codec type defines the method of voice coding and the compression mechanism that is used to convert the voice stream. The PSTN uses TDM to carry each voice call. Each voice channel reserves 64 kbps of bandwidth and uses G.711 codecs to convert the analog voice wave to a TDM voice stream. G.711 creates a 64-kbps digitized voice stream. In VoIP design, codecs compress voice beyond the 64-kbps voice stream to allow more efficient use of network resources. The most widely used codec in the WAN environment is G.729, which compresses the voice stream to 8 kbps.

Components of a VoIP Network

This topic introduces the basic components of a VoIP network.



Here are the basic components of a packet voice network:

- **IP Phones:** IP Phones provide IP voice to the desktop.
- **Gatekeeper:** The gatekeeper provides Call Admission Control (CAC), bandwidth control and management, and address translation.
- **Gateway:** The gateway provides translation between VoIP and non-VoIP networks such as the PSTN. Gateways also provide physical access for local analog and digital voice devices, such as telephones, fax machines, key sets, and PBXs.
- **Multipoint control unit (MCU):** The MCU provides real-time connectivity for participants in multiple locations to attend the same videoconference or meeting.
- **Call agent:** The call agent provides call control for IP Phones, CAC, bandwidth control and management, and address translation.
- **Application servers:** Application servers provide services such as voice mail, unified messaging, and Cisco CallManager Attendant Console.
- **Videoconference station:** The videoconference station provides access for end-user participation in videoconferencing. The videoconference station contains a video capture device for video input and a microphone for audio input. The user can view video streams and hear the audio that originates at a remote user station.

Other components, such as software voice applications, interactive voice response (IVR) systems, and softphones, provide additional services to meet the needs of enterprise sites.

VoIP Signaling Protocols

This topic describes the major VoIP protocols.

VoIP Protocol	Description
H.323	ITU standard protocol for interactive conferencing; evolved from H.320 ISDN standard; flexible, complex
MGCP	Emerging IETF standard for PSTN gateway control; thin device control
Megaco/H.248	Joint IETF and ITU standard for gateway control with support for multiple gateway types; evolved from MGCP standard
SIP	IETF protocol for interactive and noninteractive conferencing; simpler, but less mature, than H.323
RTP	IETF standard media-streaming protocol
RTCP	IETF protocol that provides out-of-band control information for an RTP flow

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0—1-8

Here are some of the major VoIP protocols:

- **H.323:** This is an ITU standard protocol for interactive conferencing. H.323 was originally designed for multimedia in a connectionless environment, such as a LAN. H.323 is an umbrella of standards that define all aspects of synchronized voice, video, and data transmission. H.323 defines end-to-end call signaling.
- **MGCP:** This is a method for PSTN gateway control or thin device control. Specified in RFC 2705, MGCP defines a protocol to control VoIP gateways that are connected to external call control devices, referred to as call agents. MGCP provides the signaling capability for less expensive edge devices, such as gateways, that may not have implemented a full voice-signaling protocol such as H.323. For example, any time an event such as off hook occurs at the voice port of a gateway, the voice port reports that event to the call agent. The call agent then signals that device to provide a service, such as dial-tone signaling.
- **H.248:** This is a joint Internet Engineering Task Force (IETF) and ITU standard that is based on the original MGCP standard. The Megaco protocol defines a single gateway control approach that works with multiple gateway applications including PSTN gateways, ATM interfaces, analog-like and telephone interfaces, IVR servers, and others. The Megaco protocol provides full call control intelligence and implements call-level features such as transfer, conference, call forward, and hold. The basic operation of the Megaco protocol is very similar in nature to MGCP; however, the Megaco protocol provides more flexibility by interfacing with a wider variety of applications and gateways.

- **SIP:** SIP is a detailed protocol that specifies the commands and responses to set up and tear down calls. SIP also details features such as security, proxy, and transport (TCP or User Datagram Protocol [UDP]) services. SIP and its partner protocols, Session Announcement Protocol (SAP) and Session Description Protocol (SDP), provide announcements and information about multicast sessions to users on a network. SIP defines end-to-end call signaling between devices. SIP is a text-based protocol that borrows many elements of HTTP, using the same transaction request and response model, and similar header and response codes. It also adopts a modified form of the URL addressing scheme used within e-mail that is based on Simple Mail Transfer Protocol (SMTP).
- **Real-Time Transport Protocol (RTP):** RTP is an IETF standard media-streaming protocol. RTP carries the voice payload across the network. RTP provides sequence numbers and time stamps for the orderly processing of voice packets.
- **Real-Time Transport Control Protocol (RTCP):** RTCP provides out-of-band control information for an RTP flow. Every RTP flow has a corresponding RTCP flow that reports statistics on the call. RTCP is used for quality of service (QoS) reporting.

VoIP Protocols and the OSI Model

This topic matches VoIP protocols to the seven layers of the Open System Interconnection (OSI) model.

VoIP Protocols and the OSI Model	
Application	Cisco SoftPhone/ Cisco CallManager/human speech
Presentation	Codecs
Session	H.323/SIP/MGCP/Megaco/H.248
Transport	RTP/UDP (media); TCP/UDP (signal)
Network	IP
Data Link	Frame Relay, ATM, Ethernet, Multilink Point-to-Point Protocol (MLP), Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC),...
Physical	...

Constant: Voice media packets use RTP/UDP
Variable: Several signaling methods and link-layer protocols

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-7

Successfully integrating connection-oriented voice traffic in a connectionless-oriented IP network requires enhancements to the signaling stack. In some ways, the user voice protocol must make the connectionless network appear more connection-oriented through the use of sequence numbers.

Applications such as Cisco IP SoftPhone and Cisco CallManager provide the interface for users to originate voice at their PCs or laptops and to convert and compress voice before passing it to the network. If a gateway is used, a standard telephone becomes the interface to users and human speech becomes the application.

Codecs define how voice is compressed. Users can configure which codec to use or negotiate a codec according to what is available.

A constant in VoIP implementation is that voice uses RTP inside UDP to carry the payload across the network. IP voice packets can reach the destination out of order and unsynchronized; the packets must be reordered and resynchronized before playing them out to the user. Because UDP does not provide services such as sequence numbers or time stamps, RTP provides the sequencing functionality.

The variables in VoIP are the signaling methods. H.323 and SIP define end-to-end call-signaling methods. MGCP and H.248 define a method to separate the signaling function from the voice call function. This last approach is referred to as client/server architecture for voice signaling. The client/server architecture uses a call agent to control signaling on behalf of the endpoint devices, such as gateways. The central control device participates in the call setup only. Voice traffic still flows directly from endpoint to endpoint.

VoIP Service Considerations

This topic describes the issues that can affect voice service in the IP network.

VoIP Service Considerations

- **Latency**
- **Jitter**
- **Bandwidth**
- **Packet loss**
- **Reliability**
- **Security**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-5

In traditional telephony networks, dedicated bandwidth for each voice stream provides voice with a guaranteed delay across the network. Because bandwidth is guaranteed in the TDM environment, there is no variable delay (jitter). Configuring voice in a data network requires network services with low delay, minimal jitter, and minimal packet loss. Bandwidth requirements must be properly calculated based on the codec that is used and the number of concurrent connections. QoS must be configured to minimize jitter and loss of voice packets. The PSTN provides 99.999 percent availability. To match the availability of the PSTN, the IP network must be designed with redundancy and failover mechanisms. Security policies must be established to address both network stability and voice-stream security.

The table lists the issues associated with implementing VoIP in a converged network and the solutions that address these issues.

Issues and Solutions for VoIP in a Converged Network

Issue	Solution
Latency	<ul style="list-style-type: none">■ Increase bandwidth■ Choose a different codec type■ Fragment data packets■ Prioritize voice packets
Jitter	<ul style="list-style-type: none">■ Use dejitter buffers
Bandwidth	<ul style="list-style-type: none">■ Calculate bandwidth requirements, including voice payload, overhead, and data
Packet loss	<ul style="list-style-type: none">■ Design the network to minimize congestion■ Prioritize voice packets■ Use codecs to minimize small amounts of packet loss
Reliability	<ul style="list-style-type: none">■ Provide redundancy for these components:<ul style="list-style-type: none">— Hardware— Links— Power (uninterruptible power supply [UPS])■ Perform proactive network management
Security	<ul style="list-style-type: none">■ Secure these components:<ul style="list-style-type: none">— Network infrastructure— Call-processing systems— Endpoints— Applications

RTP and RTCP

This topic describes the functions of RTP and RTCP as they relate to the VoIP network.

Real-Time Transport Protocol

- **Provides end-to-end network functions and delivery services for delay-sensitive, real-time data, such as voice and video**
- **Works well with queuing to prioritize voice traffic over other traffic**
- **Services include:**
 - **Payload-type identification**
 - **Sequence numbering**
 - **Time stamping**
 - **Delivery monitoring**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-1-9

RTP provides end-to-end network transport functions intended for applications transmitting real-time requirements, such as audio and video. Those functions include payload-type identification, sequence numbering, time stamping, and delivery monitoring.

RTP typically runs on top of UDP to use the multiplexing and checksum services of that protocol. Although RTP is often used for unicast sessions, it is primarily designed for multicast sessions. In addition to the roles of sender and receiver, RTP also defines the roles of translator and mixer to support the multicast requirements.

RTP is a critical component of VoIP because it enables the destination device to reorder and retime the voice packets before they are played out to the user. An RTP header contains a time stamp and sequence number, which allows the receiving device to buffer and to remove jitter and latency by synchronizing the packets to play back a continuous stream of sound. RTP uses sequence numbers to order the packets only. RTP does not request retransmission if a packet is lost.

Example: RTP Application

As voice packets are placed on the network to reach a destination, they may take one or more paths to reach their destination. Each path may have a different length and transmission speed, which results in the packets being out of order when they arrive at their destination. As the packets were placed on the wire at the source of the call, RTP tagged the packets with a time stamp and sequence number. At the destination, RTP can reorder the packets and send them to the digital signal processor (DSP) at the same pace as they were placed on the wire at the source.

Note For more information on RTP, refer to RFC 1889.

RTCP monitors the quality of the data distribution and provides control information.

Real-Time Transport Control Protocol

- **Monitors the quality of the data distribution and provides control information**
- **Provides feedback on current network conditions**
- **Allows hosts involved in an RTP session to exchange information about monitoring and controlling the session**
- **Provides a separate flow from RTP for UDP transport use**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-1-10

RTCP provides the following feedback on current network conditions:

- RTCP provides a mechanism for hosts involved in an RTP session to exchange information about monitoring and controlling the session. RTCP monitors the quality of elements such as packet count, packet loss, delay, and interarrival jitter. RTCP transmits packets as a percentage of session bandwidth, but at a specific rate of at least every 5 seconds.
- The RTP standard states that the Network Time Protocol (NTP) time stamp is based on synchronized clocks. The corresponding RTP time stamp is randomly generated and based on data packet sampling. Both NTP and RTP are included in RTCP packets by the sender of the data.
- RTCP provides a separate flow from RTP for transport use by UDP. When a voice stream is assigned UDP port numbers, RTP is typically assigned an even-numbered port and RTCP is assigned the next odd-numbered port. Each voice call has four ports assigned: RTP plus RTCP in the transmit direction and RTP plus RTCP in the receive direction.

Example: RTCP Application

Throughout the duration of each RTP call, the RTCP report packets are generated at least every 5 seconds. In the event of poor network conditions, a call may be disconnected due to high packet loss. When viewing packets using a packet analyzer, a network administrator could check information in the RTCP header including packet count, octet count, number of packets lost, and jitter. The RTCP header information would shed light on why the calls were disconnected.

Summary

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

Summary

- **The business advantages of a VoIP network include more efficient use of bandwidth, lower costs, access to advanced features, and increased revenue opportunities.**
- **Replacing the PSTN with VoIP requires the user to understand and implement appropriate use of signaling, database services, bearer control, and codec functionality.**
- **The basic components of a VoIP network include IP Phones, gateways, gatekeepers, call agents, conferencing servers, and application servers.**
- **VoIP peer-to-peer signaling protocols, such as H.323 and SIP, are most commonly used in distributed VoIP architectures.**
- **VoIP client/server signaling protocols, such as MGCP and Megaco/H.248, are most commonly used in centralized VoIP architectures.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-1-11

Summary (Cont.)

- **VoIP signaling protocols reside at the session layer of the OSI model and can operate over TCP or UDP based on their design.**
- **Issues such as latency, jitter, and packet loss are inherent in IP networks. Solutions are available to minimize the impact of these issues on voice quality.**
- **IP networks are less reliable and secure than the PSTN. Design approaches must address these issues to provide for secure transport of voice traffic with near PSTN reliability.**
- **RTP carries the voice payload and provides sequencing and time stamping to allow proper re-assembly and timing when the voice stream is played out at the receiving end.**
- **RTCP monitors the quality of voice sessions and provides feedback on current network conditions.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-1-12

References

For additional information, refer to these resources:

- RFCs. <ftp://www.ietf.org/internet-drafts/>.
- *Configuring Compressed Real-Time Protocol*.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart6/qcrtphc.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) Which three benefits pertain to packet voice networks? (Choose three.)
- A) cost savings through consolidated voice and data network expenses
 - B) automatic guaranteed delivery of digital voice
 - C) flexibility in the delivery of services
 - D) availability of advanced features to create differentiated services
 - E) reduced complexity of converged network design
 - F) reduced network protocol support by converting all applications to IP
- Q2) Which four advanced features are available in VoIP networks? (Choose four.)
- A) unified messaging
 - B) IP routing for voice packets
 - C) QoS for voice packet delivery
 - D) database services
 - E) long-distance toll bypass
 - F) H.248 signaling protocol
 - G) advance call routing
- Q3) Which two protocols are used for peer-to-peer signaling? (Choose two.)
- A) MGCP
 - B) SIP
 - C) Megaco protocol
 - D) H.248
 - E) H.323
- Q4) Bearer control reacts to which two types of messages to allocate and deallocate resources when calls are made? (Choose two.)
- A) congestion
 - B) call connect
 - C) ring tone
 - D) Call Admission Control
 - E) call disconnect

- Q5) Match the component of a packet voice network to its function.
- A) gateway
 - B) MCU
 - C) IP Phone
 - D) call agent
 - E) application server
 - F) videoconference station
- _____ 1. translates between the IP network and the PSTN
- _____ 2. provides access for end-user participation in videoconferencing
- _____ 3. brings IP voice to the desktop
- _____ 4. provides real-time connectivity for videoconferencing
- _____ 5. provides services such as voice mail and unified messaging
- _____ 6. performs call control on behalf of IP Phones
- Q6) Which two functions are provided by a gateway? (Choose two.)
- A) VLAN separation
 - B) translation between the VoIP and PSTN network
 - C) physical access for analog telephones and fax machines
 - D) power over Ethernet to the IP Phone
 - E) database services
- Q7) Which two protocols provide gateway control in a VoIP network? (Choose two.)
- A) SIP
 - B) MGCP
 - C) H.323
 - D) H.248
 - E) BGP
- Q8) Which protocol provides out-of-band control information for RTP-based call flows?
- A) RTP-Control
 - B) RTP
 - C) SNMP
 - D) RTCP
- Q9) SIP, H.323, MGCP, and H.248 work at which layer of the OSI model?
- A) application layer
 - B) session layer
 - C) transport layer
 - D) network layer
- Q10) Voice travels over which transport layer protocol?
- A) TCP
 - B) UDP
 - C) SIP
 - D) H.323

- Q11) Which two factors must be considered when you calculate bandwidth for voice connections? (Choose two.)
- A) codec
 - B) size of dejitter buffer
 - C) number of concurrent connections
 - D) distance between endpoints
 - E) type of signaling protocol used
- Q12) What must be configured in the VoIP network to minimize voice packet loss?
- A) QoS
 - B) RTP
 - C) H.323
 - D) RTCP
- Q13) RTP provides delivery services for which component?
- A) call signaling
 - B) call routing
 - C) voice payload
 - D) control information on current network conditions
- Q14) Which four conditions does RTCP monitor and report? (Choose four.)
- A) packet count
 - B) average packet size
 - C) packet loss
 - D) interarrival jitter
 - E) delay
 - F) frame errors
 - G) successful delivery of caller ID

Lesson Self-Check Answer Key

- Q1) A, C, D
Relates to: Business Case for VoIP
- Q2) A, D, E, G
Relates to: Business Case for VoIP
- Q3) B, E
VoIP Functions
- Q4) B, E
Relates to: VoIP Functions
- Q5) 1-A
2-F
3-C
4-B
5-E
6-D
Components of a VoIP Network
- Q6) B, C
Components of a VoIP Network
- Q7) B, D
Relates to: Major VoIP Protocols
- Q8) D
Relates to: Major VoIP Protocols
- Q9) B
Relates to: VoIP Protocols and the OSI Model
- Q10) B
Relates to: VoIP Protocols and the OSI Model
- Q11) A, C
Relates to: VoIP Service Considerations
- Q12) A
Relates to: VoIP Service Considerations
- Q13) C
Relates to: RTP and RTCP
- Q14) A, C, D, E
Relates to: RTP and RTCP

Lesson 2

Introducing VoIP Network Architectures

Overview

One benefit of Voice over IP (VoIP) technology is that it allows networks to be built using either a centralized or a distributed architecture. Corporate business requirements dictate the architecture and functionality that is required. This lesson discusses centralized and distributed architectures and the gateway requirements to support these architectures in enterprise and service provider environments.

Relevance

Support for protocols, signaling capabilities, voice features, and voice applications is changing and growing quickly. You must have a good understanding of voice network architectures to know which business requirements each architecture addresses. Gateways play an important role in providing access to the right mix of functionality. You must understand the main features and functions that are required in enterprise and service provider environments to choose the appropriate gateway.

Objectives

Upon completing this lesson, you will be able to describe the key components of a VoIP network in centralized and distributed architectures. This ability includes being able to meet these objectives:

- Describe how companies can build large-scale centralized network architectures using MGCP and H.248
- Describe how companies can build large-scale distributed network architectures using H.323
- Describe how companies can build large-scale distributed network architectures using SIP
- Identify the advantages and disadvantages of centralized and distributed call control
- Explain how TDM, single-protocol architecture, or protocol translation can be used to interconnect VoIP protocols

- Clarify the role of gateways that connect VoIP to traditional PSTN and telephony equipment
- List the criteria to be considered when selecting a gateway
- Identify the criteria to be considered when determining gateway interconnection requirements in an enterprise environment
- Identify the criteria to be considered when determining gateway interconnection requirements in a service provider environment

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Comprehension of telephony signaling
- Understanding the basic functions of voice gateways
- Insight into the protocol environment in which VoIP operates

Outline

The outline lists the topics included in this lesson.

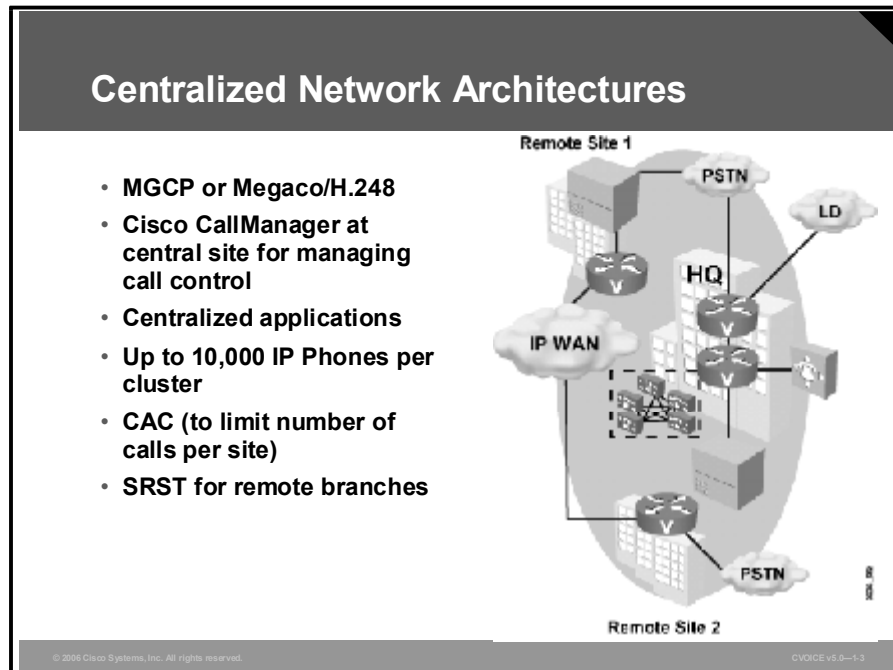
Outline

- Overview
- Centralized Network Architectures
- Distributed Network Architectures Using H.323
- Distributed Network Architectures Using SIP
- Comparing Network Architectures
- Interconnecting VoIP Protocols
- Understanding Gateways
- Guidelines for Selecting the Correct Gateway
- Enterprise Central and Remote Site Gateway Interconnection Requirements
- Service Provider Gateway Interconnection Requirements
- Summary
- Lesson Self-Check

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-2

Centralized Network Architectures

This topic describes how companies can build large, centralized network architectures using Media Gateway Control Protocol (MGCP) and H.248.



One benefit of VoIP technology is that it works with centralized and distributed architectures. This flexibility allows companies to build networks characterized by both simplified management and endpoint innovation. It is important to understand the protocols that are used to achieve this type of VoIP network agility.

The multisite WAN model with centralized call processing consists of these components:

- **Central gateway controller (call agent):** The call agent handles switching logic and call control for all sites under the central controller. A central gateway controller includes both centralized configuration and maintenance of call control functionality. When new functionality needs to be added, only the controller needs to be updated.
- **Media gateways:** Media gateways provide physical interconnection between the telephone network, individual endpoints, and the IP network. Media gateways communicate with the call agent to notify the call agent of an event. An example is a telephone going off hook. The gateway will also expect direction from the call agent regarding what action to take as a result of the event. For example, the call agent tells the gateway to provide a dial tone to the port that sees the off-hook condition. After the call control exchange is completed, the gateways route and transmit the audio or media portion of the calls. This is the actual voice information.

- **IP WAN:** The IP WAN carries both call control signaling and voice payload between the central site and the remote sites. Quality of service (QoS) configuration is highly recommended when voice packets are transported across a WAN to ensure that the voice packets get priority over data packets in the same network. To minimize bandwidth use for voice streams that are crossing the WAN, the G.729 coder-decoder (codec) is used to compress the voice payload. G.729 compresses voice to 8 kbps per call as opposed to the 64 kbps traditionally used in LAN and public switched telephone network (PSTN) environments.

A typical use for centralized architecture is a main site with many smaller remote sites. The remote sites are connected via a QoS-enabled WAN, but do not require full features and functionality during a WAN outage. MGCP and H.248 are the prevalent signaling protocols used in centralized architectures to control gateways and endpoints.

Applications such as voice mail and interactive voice response (IVR) systems are typically centralized to reduce the overall cost of administration and maintenance.

Cisco CallManager clusters can support up to 10,000 IP Phones per cluster, providing for a scalable solution in enterprise environments.

Call Admission Control (CAC) is administered by the Cisco CallManager cluster. CAC is critical in enterprise implementations that include WAN connections because these connections typically have limited bandwidth that is shared between voice and data users. Control must be established over the number of calls that can flow concurrently across the WAN at any given time so that as the call volume grows, overall call quality does not diminish.

One disadvantage of implementing a centralized architecture is that if the WAN connection fails between the remote site and the central site that houses Cisco CallManager, no further voice calls can be processed by the remote site. Additional steps need to be taken to ensure that data and voice services at the remote sites remain available. One option is to implement redundant WAN links between the remote sites and the central site. In many cases, this solution is not financially feasible. Survivable Remote Site Telephony (SRST) provides high availability for voice services. SRST provides a subset of the call-processing capabilities within the remote office gateway. SRST also enhances the IP Phones with the ability to re-home to the call-processing functions in the local gateway if a WAN failure is detected. This feature allows the remote site to continue to provide voice connectivity in the absence of the WAN link.

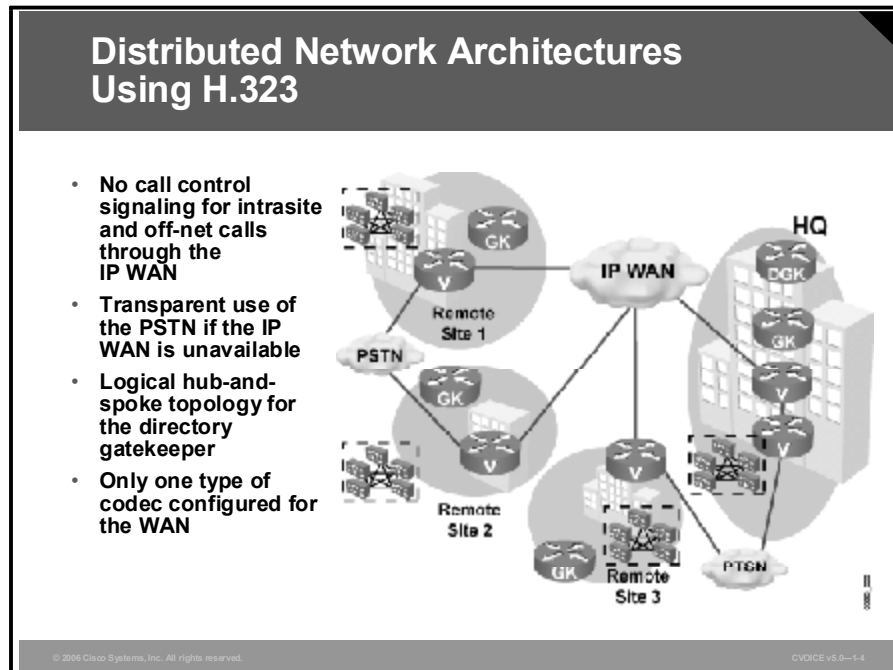
Most centralized VoIP architectures use MGCP or H.248 protocols. You can also build session initiation protocol (SIP) or H.323 networks in a centralized fashion. This is done using back-to-back user agents (B2BUAs) or Gatekeeper-Routed Call Signaling (GKRCS), respectively.

Example: Centralized Network Architectures

The figure shows a typical centralized call-processing deployment, with a Cisco CallManager cluster as the call agent at the central site and an IP WAN with QoS enabled to connect all the sites. The remote sites rely on the centralized Cisco CallManager cluster to handle their call processing but have local voice-enabled routers to perform the voice gateway translations for media streams. Each remote site connects locally to the PSTN. Long-distance service may be provided from the head office or through each local PSTN connection.

Distributed Network Architectures Using H.323

This topic describes how companies can build large distributed network architectures using H.323.



The multisite WAN architecture with distributed call processing consists of multiple independent sites. Each site has its own call-processing agent, which is connected to an IP WAN that carries voice traffic between the distributed sites.

Each site in the distributed call-processing architecture can comprise one of the following:

- A single site with its own call-processing agent
- A centralized call-processing site and all its associated remote sites
- A legacy PBX with a VoIP gateway

Multisite distributed call processing allows each site to be completely self-contained. The IP WAN in this model does not carry call control signaling for intranet and off-net calls because each site has its own Cisco CallManager cluster. 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.

Distributed architectures are associated with H.323 and SIP protocols. These protocols allow network intelligence to be distributed between endpoints and call control devices. Intelligence in this instance refers to call state, calling features, call routing, provisioning, billing, or any other aspect of call handling. The endpoints can be VoIP gateways, IP Phones, media servers, or any device that can initiate and terminate an H.323 VoIP call. The call control devices are called gatekeepers in an H.323 network. In an enterprise environment where many gatekeepers are required, a second level of hierarchy is achieved through the use of directory gatekeepers. Directory gatekeepers provide summarization capabilities for multiple configured gatekeepers.

The figure shows components, call signaling, and call flows associated with an H.323 enterprise network.

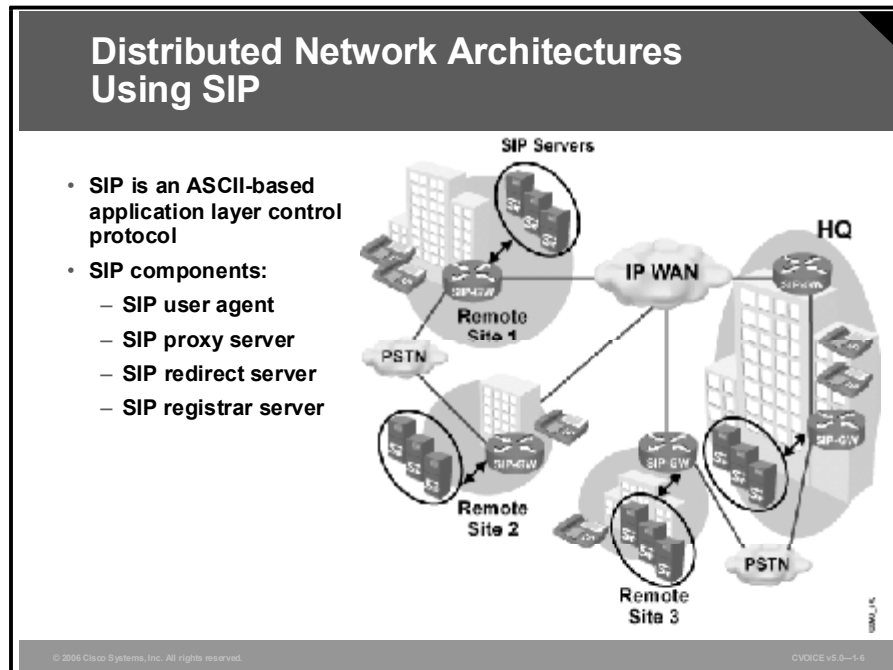
The multisite WAN architecture with distributed call processing consists of these components:

- **Media gateways:** Media gateways provide physical interconnection between the telephone network, individual endpoints, and the IP network. The media gateway translates call signaling between the PSTN or local endpoints and the IP network. The media gateway must contain the call-processing intelligence to perform all call-handling functions related to H.323. Media gateways communicate with gatekeepers for call address resolution and CAC.
- **Gatekeeper:** A gatekeeper is an H.323 device that provides CAC and E.164 dial plan resolution. Gatekeepers are among the key elements in the multisite WAN model that have distributed call processing. Gatekeepers provide dial plan resolution, which improves scalability in an H.323 network. Without gatekeepers, each gateway would need to be configured to know where all other reachable telephone numbers were located. The gatekeeper provides a central repository of telephone numbers and the gateways associated with those numbers. When the network is configured for gatekeepers, the learning process is dynamic because all participating gateways register with the gatekeeper and notify it of available telephone numbers. The gatekeeper also provides CAC to ensure that voice quality is not diminished when a large number of calls enter the network.
- **IP WAN:** The IP WAN carries call control signaling and voice payload for intersite voice communication only. Call signaling and voice transmission for all intrasite calls and off-net calls that are going to the local PSTN remain local to the site. QoS configuration is highly recommended when voice packets are transported across a WAN to ensure that the voice packets get priority over data packets in the same network. As in the centralized system, to minimize bandwidth use for voice streams that are crossing the WAN, the G.729 codec is used to compress the voice payload. G.729 compresses voice to 8 kbps per call as opposed to the 64 kbps that is traditionally used in LAN and PSTN environments.

Few implementations of call control are totally distributed. Although H.323 and SIP operate in a purely distributed mode, for scalability reasons, both are most often deployed with common control components that give endpoints many of the advantages of a centralized call control environment. Unfortunately, these implementations also inherit many of the disadvantages of centralized call control.

Distributed Network Architectures Using SIP

This topic describes how companies can build large distributed network architectures using SIP.



The rapid evolution of voice and data technology is significantly changing the business environment. The introduction of services, such as instant messaging, integrated voice and e-mail, and follow-me services, has contributed to a work environment where employees can communicate much more efficiently, thus increasing productivity. To meet the demands of the changing business environment, businesses are beginning to deploy converged voice and data networks based on SIP.

SIP was originally defined in 1999 by the Internet Engineering Task Force (IETF) in RFC 2543. SIP is the IETF standard for multimedia conferencing over IP. SIP is an ASCII-based, application layer control protocol that can be used to establish, maintain, and terminate calls between two or more endpoints. Service development in the SIP environment is made easier because of its use of, and similarity to, Internet technologies such as HTTP, Domain Name System (DNS), and addressing in the form of e-mail addresses. SIP enables the integration of traditional voice services with web-based data services, including self-based provisioning, instant messaging, presence, and mobility services.

A SIP-based network is made up of these components:

- **SIP user agent (UA):** A SIP UA is any network endpoint that can originate or terminate a SIP session. This device could be a SIP-enabled telephone, a SIP PC client (known as a softphone), or a SIP-enabled gateway.
- **SIP proxy server:** This is a call control device that provides many services, such as routing of SIP messages between SIP UAs.
- **SIP redirect server:** This is a call control device that provides routing information to UAs when requested, giving the UA an alternate uniform resource identifier (URI) or destination user agent server (UAS).
- **SIP registrar server:** This is a device that stores the logical location of UAs within that domain or subdomain. A SIP registrar server stores the location of UAs and dynamically updates its data via REGISTER messages.

SIP provides these 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:** Via Session Description Protocol (SDP), SIP determines the “lowest level” of common services between the endpoints. Conferences are established using only those 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 already on the phone or did not answer in the allotted number of rings. SIP then returns a message that indicates why the target endpoint was unavailable.
- **Establishes a session between the originating and target endpoint:** 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. Then SIP terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

As a protocol used in a distributed architecture, SIP allows companies to build large networks that are scalable, resilient, and redundant. SIP provides mechanisms for interconnecting with other VoIP networks and for adding intelligence and new features on either the endpoints or the SIP proxy or redirect servers.

Comparing Network Architectures

To select the network architecture that best fulfills your needs, you must understand the differences in call control between centralized and distributed network architectures. This topic compares the advantages and disadvantages of centralized and distributed call control.

Centralized Call Control vs. Distributed Call Control	
Centralized Call Control	Distributed Call Control
Centralized administration	Distributed administration
Ease of dial plan consistency and updating	Dial plan consistency and updating more difficult
Supplementary services (PBX features)	Supplementary services harder to implement
Difficult to scale; all new features and applications must be implemented on central controller, central breakpoint, or bottleneck	Scalable; Need more applications, hardware or performance; add more servers, and they can be located anywhere
Challenging to provide resiliency over network failures	Resilient over network failures
Difficult to add new endpoints and applications; elements are tightly associated	Conceptually easy to add new endpoints and applications
WAN-inefficient	WAN-efficient
Dial delay bears no relation to distance between endpoints	Dial delay roughly proportional to the distance between the endpoints, as in the public switched telephone network (PSTN)
Static endpoint capabilities	Flexible; Negotiation of endpoint capabilities per session

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0-17

The figure shows a comparison of the centralized and distributed call control models. Both models have advantages and disadvantages. Features that are considered advantages of one type of call control model may be disadvantages of the other type. The main differences between the two models are in these areas:

- Configuration:** The centralized call control model provides superior control of the configuration and maintenance of the dial plan and endpoint database. It simplifies the introduction of new features and supplementary services. The centralized call control model also provides a convenient location for the collection and dissemination of CDRs (Call Detail Records).

The distributed model requires distributed administration of the configuration and management of endpoints. This approach complicates the administration of a dial plan. Distributed call control simplifies the deployment of additional endpoints while making new features and supplementary services difficult to implement.

- Security:** Centralized call control requires that endpoints be known to a central authority. This approach avoids or reduces security concerns.

The autonomy of endpoints in the distributed model elevates security concerns.

- Reliability:** The centralized model has two points of vulnerability: single point of failure and contention. The centralized model places high demands on the availability of the underlying data network, necessitating a fault-tolerant WAN design.

The distributed call control model minimizes the dependence on shared common control components and network resources. This approach reduces exposure to single point of failure and contention for network resources.

- **Efficiency:** Centralized call control fails to take full advantage of computer-based technology that resides in the endpoints. It also consumes bandwidth through the interaction of the call agent and its endpoints.

Distributed call control takes advantage of the inherent computer-based technology in endpoints.

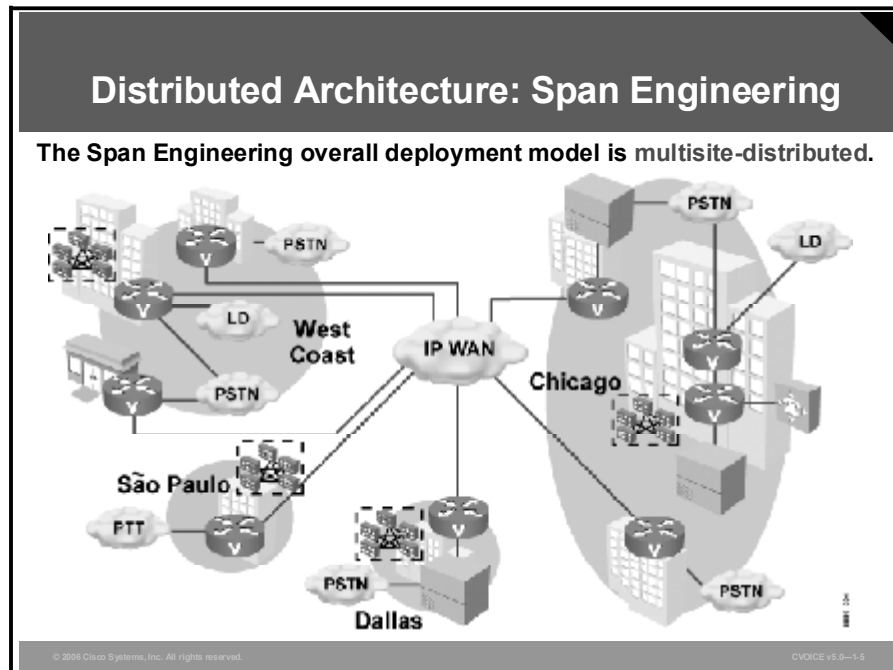
Example: Comparing Centralized and Distributed Call Control Models

Because the centralized model increases vulnerability, it mandates the implementation of survivability and load management strategies that involve the replication of the central components. Few implementations of call control are totally distributed. For example, H.323 and SIP operate in a purely distributed mode; however, for scalability reasons, both H.323 and SIP are most often deployed with common control components that give endpoints many of the advantages of a centralized call control environment. Unfortunately, these implementations also inherit many of the disadvantages of centralized call control.

Example: Simple Multisite IP Telephony Network

Span Engineering LLC is a company based in the United States, with headquarters in Chicago and branches in Dallas and on the West Coast. The company has recently expanded internationally to São Paulo, Brazil. Span Engineering is migrating to a Cisco IP telephony solution. The plan for migrating to Cisco IP telephony includes eliminating all PBXs and migrating to full VoIP in the near future.

This diagram shows the distributed architecture implemented by Span Engineering.



The overall deployment model used by Span Engineering is multisite-distributed and contains both centralized and single-site locations.

- **Centralized call control (Chicago):** Span Engineering has three separate locations in Illinois, with the Chicago location serving as the headquarters. A centralized network architecture is used for the Illinois sites. The Cisco CallManager cluster in Chicago manages call address resolution and CAC for the three Illinois locations.
- **Centralized call control (West Coast):** Span Engineering has recently acquired three West Coast companies. The companies consist of a 12-story location in San Francisco, a 2-story location in Oakland, and a single-story location in San Jose. The San Francisco location houses the Cisco CallManager cluster that serves all three West Coast locations.
- **Single-site call control (São Paulo and Dallas):** Span Engineering currently has no plans to expand in these locations but wants to ensure high availability of voice communication capabilities. The company has chosen to put Cisco CallManager clusters in each of these locations as single-site locations. Both the Dallas and São Paulo sites have local connections to telephone service providers for local dial tone. In non-North American countries, the telephone service provider is referred to as the Post, Telephone, and Telegraph (PTT) provider.

Note You will be using the Span Engineering example throughout this course to help you understand VoIP implementations.

Interconnecting VoIP Protocols

This topic describes the choices that companies have for interconnecting VoIP protocols, including translation through time-division multiplexing (TDM), single-protocol architecture, and protocol translation.

Interconnecting VoIP Protocols	
Method	Description
Translation through TDM	<ul style="list-style-type: none">• VoIP1 -> TDM -> VoIP2• Widely available• Adds latency
Single-protocol architecture	<ul style="list-style-type: none">• Migrates all devices and services to single VoIP protocol• Limits flexibility
Protocol translation	<ul style="list-style-type: none">• VoIP -> translator -> VoIP2• Lack of standards for protocol translation

© 2006 Cisco Systems, Inc. All rights reserved. CHOICE v3.0-1.8

Just as companies choose various protocols for their data networks based on business and technical requirements, they also need to choose one or more protocols for their VoIP requirements. In an environment where more than one VoIP protocol is present, companies must support the interconnection between differing VoIP protocols.

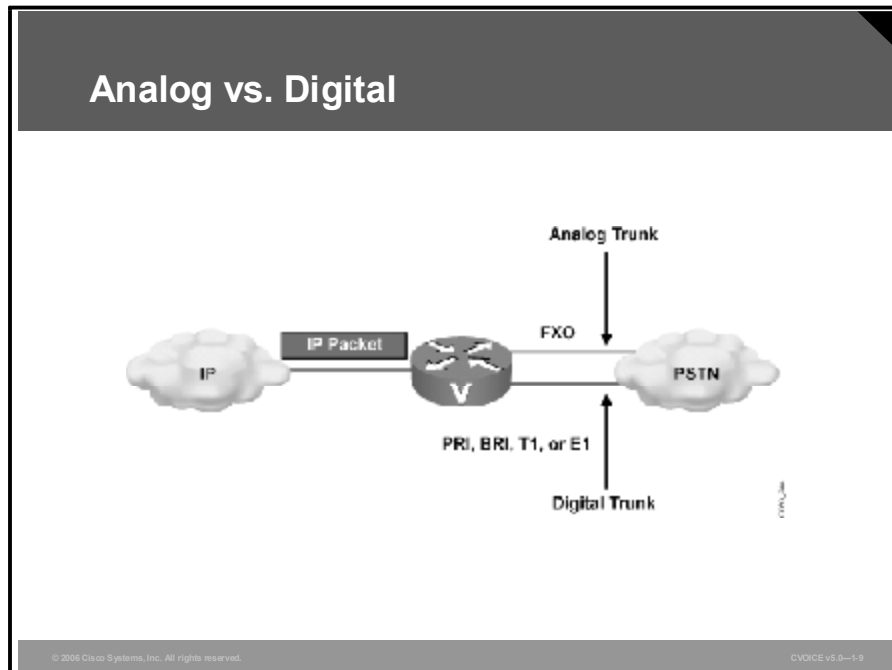
Choices for interconnecting the segments that use differing VoIP protocols typically fall into one of these three categories:

- **Translation through TDM:** In this method, a company uses either TDM equipment or VoIP gateways to translate from one protocol domain to another. The benefit of this method is the widespread availability of devices that provide this translation. The downside is that this method introduces latency into the VoIP network and introduces an additional translation (TDM) into the voice path between two protocol domains. This method is usually considered a short-term solution until VoIP translators become available.
- **Single-protocol architecture:** In this method, a company moves all its VoIP devices and services to a single protocol, simplifying the network as a whole. The downside to this approach is that it might not be possible to migrate existing equipment to support the new protocol. This situation can limit the ability of the company to take advantage of some existing services. In addition, this method limits the potential connectivity to other networks that are using other VoIP signaling protocols.

- **Protocol translation:** In this method, a company uses IP-based protocol translators to interconnect two or more VoIP protocol domains. IP translators allow a company to retain the flexibility of using multiple VoIP protocols. They do not introduce the delay problems that additional TDM interconnections do. IP translators also do not require the wholesale replacement of existing equipment. The negative aspect of this approach is that there is no standard for protocol translation. Not all VoIP protocol translators are exactly the same. Although the IETF attempted to define a model for translating H.323 to SIP, this model involves more than just building a protocol translation box. Vendors of protocol translators need in-depth knowledge of all the protocols that are being used in the VoIP network. These vendors must be aware of how various VoIP components use different aspects of the protocol. For example, H.323 and SIP can send dual-tone multifrequency (DTMF) digits in either the signaling path or the media path via Real-Time Transport Protocol (RTP). H.323 mandates only that the H.245 signaling path be used. SIP does not specify how DTMF should be carried. This design means that SIP devices could be sending DTMF in the media path (RFC 2833), and H.323 devices could be sending DTMF in the signaling path (H.245). If the VoIP protocol translator cannot properly recognize both the signaling path and the media path, the protocol translator may not function properly.

Understanding Gateways

This topic describes the role of gateways in connecting VoIP to traditional PSTN and telephony equipment.



A gateway is a device that translates one type of signal to a different type of signal. There are different types of gateways, including voice gateways.

A voice gateway is a router or switch that converts IP voice packets to analog or digital signals that are understood by TDM trunks or stations. Gateways are used in several situations; for example, to connect the PSTN, a PBX, or a key system to a VoIP network.

Example: Analog and Digital Gateways

In the figure, the voice-enabled router examines the incoming IP packet to determine if it is a voice packet and where it is heading. Based on information inside the voice packet, the router translates the digitized signal or voice into the appropriate analog or digital signal to be sent to the PSTN. For a call coming from the PSTN, the gateway interprets the dialed digits and determines the IP destination for this call.

Guidelines for Selecting the Correct Gateway

This topic describes the criteria to be considered when selecting a gateway.

Gathering the Requirements

- **Is an analog or digital gateway required?**
- **What is the required capacity of the gateway?**
- **What type of connection is the gateway going to use?
Is Foreign Exchange Office (FXO), FXS, E&M, T1, E1, PRI,
or BRI signaling required?**
- **What signaling protocol is used? H.323, MGCP, or SIP?**
- **Is voice compression a part of the design? If so, which type?**
- **Are direct inward dialing (DID), calling line ID (CLID), modem relay,
or fax relay required?**
- **Is the device acting only as a gateway or as a gateway and a
router/LAN switch? Is inline power for IP Phones required?**
- **Is remote site survivability required?**
- **To which country is the hardware shipped?**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0--110

Understanding gateways and being able to select the correct gateway out of numerous gateway options is challenging. Factors to consider include the protocols that are supported, the density and types of interfaces on the gateway, and the features that are required. Knowing the requirements will guide you to the correct solution.

One criterion involves defining the type of site that the gateway supports. Is it a small office/home office (SOHO), branch office, enterprise campus environment, or service provider? Each type of site has its own set of requirements.

The figure lists the questions that you should ask before selecting a gateway. The answers will help to define the gateway functions. You will also be able to determine if the proposed design meets current requirements and encompasses future growth.

A key objective is to identify the number and type of voice interfaces that are necessary and verifying the protocol support. Are supplementary services supported? Which codecs must be supported? Is fax relay necessary? Many of these functions are features of specific Cisco IOS software releases. Identification of the proper IOS software release that is necessary to support the features is critical.

Another key question is whether the gateway is acting as a gateway only or needs to combine the functions of gateway and router within one device. This will point to a specific set of hardware and software.

When planning gateways for locations in other countries, verify that the device meets the government standards for PSTN connection in that country. If the device supports encryption capabilities, verify the legality of export to the destination country.

Example: Selecting a Gateway

The requirements for selecting a gateway are to support Foreign Exchange Station (FXS) and E&M connections. The trunk is to be a T1 PRI from the PBX. In this case, a suitable choice would be a Cisco 3745 Multiservice Access Router with a two-slot voice network module (VNM), one FXS voice interface card (VIC), one E&M VIC, and a High Density Voice (HDV) module.

Enterprise Central and Remote Site Gateway Interconnection Requirements

This topic describes the criteria to be considered when determining gateway interconnection requirements in an enterprise environment.

Remote Site Enterprise Gateway Considerations

- **QoS capabilities for voice quality**
- **Security to ensure privacy of communications over the WAN**
- **Appropriate number and type of voice interfaces and features**
- **Survivability of telephone service in the event of a WAN outage**
- **Analog and digital fax/modem capabilities**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0—1-11

As IP telephony services become a standard in the corporate setting, a broad mix of requirements surface in the enterprise environment. The IP telephony deployment is typically initiated by connecting to the PSTN to manage off-net calls while using a Cisco CallManager infrastructure to manage on-net calls.

Example: Gateway Interconnect Considerations

The table shows examples of questions that you must ask to determine the requirements for gateway interconnections.

Determining Gateway Interconnection Requirements

Question	Reasoning
How do you control the gateways?	You must ensure support for proper call processing, such as MGCP, SIP, or H.323.
Is cost an issue?	Distributed call processing is easier to implement, but the costs are higher when deploying intelligent devices at each site.
Is remote site survivability an issue?	Remote site survivability is not an issue with a distributed model unless there is a need for redundancy. This is an issue for a centralized model that must be addressed by providing SRST. This means ensuring that the version of Cisco IOS software supports the feature.
Are gatekeepers in the design, and if so, how are the zones structured?	Gatekeepers are normally used in enterprise sites for scalability and manageability. The design must include proper planning for zone configurations.
Are the gateways switches or routers?	This question determines how other features, such as QoS, are implemented. Numerous switches and routers are available that have voice gateway functionality along with other core services. These services include Layer 2 and Layer 3 QoS implementations, inline power, and security features.
Is fax or modem support required?	Is the gateway capable of fax and modem relay functions? An alternative for the enterprise customer is to purchase IP telephony services from a service provider. In that case, a decision must be made regarding who manages the gateway and what type of connection is required. For example, the customer might choose SIP, H.323, or MGCP.

Central Site Enterprise Gateway Considerations

- **Dial plan integration**
- **Voice-mail integration**
- **Gateway for PBX interconnect**
- **Inline power requirements for IP Phones**

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-1-12

At the central site, these specific issues need to be addressed:

- **Dial plan integration:** Consistent reachability demands that the new dial plan for the IP voice network must integrate with the existing dial plan. It is essential that you have a thorough understanding of how the dial plans interact.
- **Voice-mail integration:** After a voice-mail application is selected, the designer must ensure that all users can seamlessly reach the voice-mail server. It is also vital that all incoming calls are properly forwarded when the recipient does not answer the telephone. This may mean dedicating gateway connections for an existing voice-mail server, or dedicating an entire gateway for the express purpose of voice-mail server integration.
- **Gateway for PBX interconnect:** When the IP voice network interconnects PBXs, the designer must determine which type of connection is supported by the PBX and which gateway will support that connection.
- **Inline power requirements for IP Phones:** When the design includes IP Phones, the power requirements must be considered. In many cases, it is desirable to provide inline power to the telephones. A number of devices provide inline power. The decision about inline power requirements is based on capacity and the current power options.

Note The network administrator should evaluate the need for inline power based on the network design.

Service Provider Gateway Interconnection Requirements

This topic describes the criteria to be considered when determining gateway interconnection requirements in a service provider environment.

Service Provider Gateway Considerations

- **Signaling interconnection type**
 - SS7 supports a high volume of call setup.
- **Carrier-class performance**
 - Gateways must have redundancy and QoS support.
- **Scalability**
 - Gateways must support rapid growth.

© 2006 Cisco Systems, Inc. All rights reserved. VOICEv5.0-1-13

Service providers must provide a level of service that meets or exceeds PSTN standards. The gateways that service providers implement must provide for reliable, high-volume voice traffic with acceptable levels of latency and jitter. The following functions address those requirements:

- **Signaling interconnection type:** Signaling System 7 (SS7) interconnect supports a high volume of call setup and benefits from redundant interconnect capabilities directly into the PSTN switch network.
- **Carrier-class performance:** Carrier-class performance can be provided through the proper redundant design for high availability in addition to the proper implementation of QoS features to ensure acceptable delay and jitter.
- **Scalability:** Scalability is a critical factor in the service provider arena. Customers who need access should be serviced promptly. Choosing a gateway with capacity for rapid growth is an important design decision. Gateways can scale upward to T3 capabilities for large-scale environments.

Example: Service Provider Requirements

An IP telephony service provider needs to upgrade its existing gateway platforms because of business growth. The service provider sells a managed IP telephony service to small and midsize businesses and provides connections to many different low-cost, long-distance carriers. Their issues are call quality over the IP network. Delay and jitter need to be controlled. Service providers also must consider scalability and the ability to provide differentiated levels of service through QoS. They also need connectivity to the SS7 networks of long-distance carriers to reduce costs. Finally, they need to consider the overall cost of implementation. SS7 capabilities and a redundant design enable the service provider to deliver a reliable level of service.

Practice Item: Network Architecture

Span Engineering is assessing VoIP network architectures and reviewing components and functionality associated with each type of architecture. Your task is to view each scenario and determine the network architecture type and the protocols that are commonly used in support of the network architecture.

Scenario 1

Based on this diagram, identify the network architecture type and protocols that are commonly used to support that architecture.

Practice Item: Scenario 1

- Cisco CallManager acts as the call agent.
- The voice gateway provides physical connectivity for end devices.
- The voice gateway does not contain full call-signaling protocol implementation.
- The call agent manages voice gateways.
- Call control signaling for all calls crosses the IP WAN.
- CAC limits the number of calls per site.
- SRST is used for remote branches.

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-14

Network architecture: _____

Protocols: _____

Scenario 2

Based on this diagram, identify the network architecture type and protocols that are commonly used to support that architecture.

Practice Item: Scenario 2

- The voice gateway provides physical connectivity for end devices.
- The voice gateway has the functionality to perform call setup and teardown.
- Gatekeepers are used to provide call control.
- Gatekeepers provide a scalable approach to dial plan resolution.
- There is no call control signaling for intrasite and off-net calls through the IP WAN.

© 2006 Cisco Systems, Inc. All rights reserved. VOICEv5.0-1-15

Network architecture: _____

Protocols: _____

Practice Item Answer Key

Scenario 1

Network architecture: Centralized

Protocols: MGCP and H.248

Scenario 2

Network architecture: Distributed

Protocols: H.323

Summary

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

Summary

- **Centralized network architectures use MGCP or Megaco/H.248 to provide enterprise-wide gateway control from a central controller.**
- **Distributed network architectures require gateways and endpoints to contain the intelligence necessary to perform call control functions using H.323 or SIP.**
- **SIP networks allow companies to build large-scale networks and provide flexibility to integrate to web-based applications.**
- **Selection of the appropriate network architecture requires a thorough understanding of the differences in call control between architectures.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-1-16

Summary (Cont.)

- **Choices for interconnecting differing VoIP networks include translation through TDM, migrating to a single-protocol environment, or using protocol translators.**
- **A voice gateway converts voice packets to analog or digital signals.**
- **When you are selecting a gateway, you must consider what protocols are supported, the density and types of interfaces on the gateway, and the features that are required.**
- **Enterprise interconnection design issues include distributed versus centralized call processing, SRST, QoS, and fax/modem relay requirements.**
- **Service provider interconnection requirements typically include use of SS7 to signal the PSTN, carrier-class performance, and scalability.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-1-17

References

For additional information, refer to these resources:

- *Product Bulletin, No. 1596: Cisco IOS Software Release 12.2(4)XW.*
http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/1596_pp.htm.
- *IP Telephony/Voice over IP (VoIP): Understanding Packet Voice Protocols.*
http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a008009294d.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) A company has four sites and wants to implement VoIP at all of them. The requirements include implementing gateway devices with no call-processing intelligence at the remote sites, controlling all call traffic from the headquarters location, and having a single point of CAC. Which network architecture is appropriate for these requirements?
- A) single-site architecture
 - B) distributed architecture
 - C) centralized architecture
 - D) H.323 gateway architecture
- Q2) Which two protocols can be used to control gateways in a centralized architecture environment? (Choose two.)
- A) H.248
 - B) SIP
 - C) H.323
 - D) RSVP
 - E) MGCP
 - F) SCCP
- Q3) Which condition best describes call-processing intelligence in a distributed network architecture?
- A) Gateways at each site contain the call-processing intelligence necessary to set up, maintain, and tear down voice calls.
 - B) Gateways at each site provide physical connectivity only; connected end devices contain all call-processing intelligence.
 - C) Gateways at each site provide physical connectivity only; gateways query a call agent to determine event responses.
 - D) Gateways are not required in a distributed network architecture because Cisco CallManager performs all call-processing functions.
- Q4) Which two protocols are typically used in a distributed network architecture? (Choose two.)
- A) H.248
 - B) SIP
 - C) H.323
 - D) RSVP
 - E) MGCP
 - F) SCCP
- Q5) Which description best depicts the use of a gatekeeper in a distributed network environment?
- A) The gatekeeper provides connectivity for analog telephones and fax machines.
 - B) The gatekeeper controls call processing on behalf of the gateway.
 - C) The gatekeeper translates voice streams between differing voice protocols.
 - D) The gatekeeper provides CAC and dial plan resolution.

- Q6) Match each SIP component to the functionality that it provides.
- A) SIP user agent
 - B) SIP proxy server
 - C) SIP redirect server
 - D) SIP registrar server
- _____ 1. a call control device that provides routing information to user agents when requested, giving the user agent an alternate URI or destination UAS
- _____ 2. a call control device that provides many services such as routing of SIP messages between SIP user agents
- _____ 3. a device that stores the logical location of user agents within that domain or subdomain
- _____ 4. any network endpoint that can originate or terminate a SIP session; for example, a SIP-enabled telephone, a SIP PC client, or a SIP-enabled gateway
- Q7) What are two advantages of a distributed call control model? (Choose two.)
- A) superior configuration control
 - B) fault tolerance
 - C) simplified introduction of new features
 - D) simplified deployment of additional endpoints
 - E) superior maintenance of the endpoint database
- Q8) What are two advantages of a centralized call control model? (Choose two.)
- A) minimized dependence on network resources
 - B) superior maintenance of the dial plan
 - C) simplified introduction of supplementary services
 - D) simplified deployment of additional endpoints
 - E) reduced bandwidth consumption
- Q9) Which reason best describes why SIP gives companies the ability to easily build new services and integrate traditional voice services with new web-based services?
- A) SIP is a mature protocol that has been used in traditional telephony for the past decade and is well understood in the telephony environment.
 - B) SIP is a session layer protocol that is supported by default on all VoIP devices.
 - C) SIP is an ASCII-based, application layer protocol that uses existing Internet standards and is easily understood.
 - D) SIP is widely used by all PSTN providers.
- Q10) In a multiprotocol VoIP environment, what benefit does translation through TDM provide?
- A) decreases latency
 - B) uses less bandwidth than direct translation between protocols
 - C) is widely available
 - D) does not require configuration

- Q11) There are three methods for interconnections in a multiprotocol environment. Match each interconnection method to the disadvantages associated with its use.
- A) translation through TDM
 - B) single-protocol architecture
 - C) protocol translation
- _____ 1. lack of translation standards
- _____ 2. limited flexibility
- _____ 3. added latency
- Q12) In which of these situations would a gateway be required?
- A) a Cisco CallManager-to-IP network connection
 - B) a PBX-to-voice mail connection
 - C) a key system-to-IP network connection
 - D) a PBX-to-PBX connection
- Q13) The gateway translates the digitized signal or voice into the appropriate analog or digital signal for the PSTN, based on which of these factors?
- A) configuration of the gateway
 - B) protocols being used on the network
 - C) default settings of the gateway
 - D) information inside the voice packet
- Q14) When a call arrives from the PSTN, how does the gateway know where to send the call?
- A) from the IP address included in the call
 - B) from the dialed digits in the call
 - C) from the calling digits included in the call
 - D) from the CLID information in the call
- Q15) What are two reasons why it is important to know which country the gateway will be located in when you are planning a network? (Choose two.)
- A) network requirements
 - B) standards for PSTN connections
 - C) design requirements
 - D) functions required of the gateway
 - E) legal issues involving encryption services
- Q16) Which three signaling protocols can be used with gateways? (Choose three.)
- A) H.323
 - B) MGCP
 - C) SIP
 - D) SCCP
 - E) Megaco protocol

- Q17) Which two issues need to be addressed when selecting a gateway for an enterprise central site? (Choose two.)
- A) signaling interconnection type
 - B) carrier-class performance
 - C) scalability
 - D) inline power requirements for IP Phones
 - E) dial plan integration
 - F) voice-mail integration
- Q18) Why is it important to determine if the gateways are switches or routers?
- A) It dictates how many gateways to deploy.
 - B) It determines how QoS, inline power, and security features are to be implemented.
 - C) It affects zone configurations.
 - D) It determines the Cisco IOS software release that should be used.
- Q19) Which three features will influence the type of gateway that will be required for an enterprise remote site? (Choose three.)
- A) the routing protocol that the LAN and WAN need to support
 - B) the type of QoS required
 - C) the number of analog phones or modems that will need support
 - D) the level of security that will need to be supported
 - E) the type of network management that will need to be supported
- Q20) Which three features need to be considered when selecting a gateway for a service provider network? (Choose three.)
- A) high-volume call setup
 - B) high availability
 - C) scalability
 - D) SIP support
 - E) interoperability with customer applications
- Q21) If implemented properly, which two features of a service provider gateway can provide carrier-class performance? (Choose two.)
- A) scalability
 - B) redundant design planning
 - C) prompt service for customers
 - D) implementation of QoS features
 - E) support for a high volume of call setup

Lesson Self-Check Answer Key

- Q1) C
Relates to: Centralized Network Architectures
- Q2) A, E
Relates to: Centralized Network Architectures
- Q3) A
Relates to: Distributed Network Architectures
- Q4) B, C
Relates to: Distributed Network Architectures
- Q5) D
Relates to: Distributed Network Architectures
- Q6) 1-C
2-B
3-D
4-A
Relates to: Distributed Network Architectures Using SIP
- Q7) B, D
Relates to: Comparing Network Architectures
- Q8) B, C
Relates to: Comparing Network Architectures
- Q9) C
Relates to: Distributed Network Architectures
- Q10) C
Relates to: Interconnecting VoIP Protocols
- Q11) 1-C
2-B
3-A
Relates to: Interconnecting VoIP Protocols
- Q12) C
Relates to: Understanding Gateways
- Q13) D
Relates to: Understanding Gateways
- Q14) B
Relates to: Understanding Gateways
- Q15) B, E
Relates to: Guidelines for Selecting the Correct Gateway
- Q16) A, B, C
Relates to: Guidelines for Selecting The Correct Gateway

- Q17) E, F
Relates to: Enterprise Central and Remote Site Gateway Interconnection Requirements
- Q18) B
Relates to: Enterprise Central and Remote Site Gateway Interconnection Requirements
- Q19) B, C, D
Relates to: Enterprise Central and Remote Site Gateway Interconnection Requirements
- Q20) A, B, C
Relates to: Service Provider Gateway Interconnection Requirements
- Q21) B, D
Relates to: Service Provider Gateway Interconnection Requirements

Lesson 3

Building Scalable Dial Plans

Overview

This lesson describes the attributes of numbering plans and scalable dial plans for voice networks, addresses the challenges of designing these plans, and identifies the methods of implementing dial plans.

Relevance

To integrate Voice over IP (VoIP) networks into existing voice networks, network administrators must have the skills and knowledge to implement a scalable numbering plan and a comprehensive, scalable, and logical dial plan.

Objectives

Upon completing this lesson, you will be able to develop scalable dial plans to meet both domestic and overseas requirements. This ability includes being able to meet these objectives:

- Differentiate between numbering and dial plans
- Describe the advantages and attributes of a hierarchical numbering plan, including simplified provisioning, simplified routing, summarization, scalability, and management
- Recognize the characteristics of external PSTN numbering schemes in various countries, including varying number lengths, specialized services, voice mail, use of prefixes or area codes, and international dialing considerations that affect numbering planning
- Explain why VoIP dial plans must be comprehensive and scalable, using a typical North American Centrex deployment as an example
- Discuss the benefits of adhering to the required attributes of a scalable dial plan, including logic distribution, hierarchical design, simplicity in provisioning, reduction of postdial delay, and availability and fault tolerance
- Determine how number normalization and technology prefixes are used to integrate existing dial plans into a VoIP network
- Identify how VoIP operators can provide the location and telephone number of mobile callers to 911 operators

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Basic Knowledge of VoIP networks
- Basic knowledge of telephone numbering plans, such as E.164

Outline

The outline lists the topics included in this lesson.

Outline

- Overview
- Numbering and Dial Plans
- Hierarchical Numbering Plans
- Internal Numbering and Public Numbering Plan Integration
- Scalable Dial Plans
- Scalable Dial Plan Attributes
- Enhancing and Extending an Numbering Existing Plan to Accommodate VoIP
- Accounting for Caller Mobility for 911 Services
- Summary
- Lesson Self-Check

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-1-2

Numbering and Dial Plans

This topic describes the difference between a numbering plan and a dial plan.

Numbering and Dial Plans

- **Numbering plans assign telephone numbers to end devices or applications for current needs and future growth.**
- **Dial plans consist of summarized dialing patterns based on the implemented numbering plan. Dial plans may include use of access codes, area codes, specialized codes, and combinations of the numbers of digits that are dialed.**
- **Dial plans address overlapping number ranges through the use of site access codes.**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v9.0-1-3

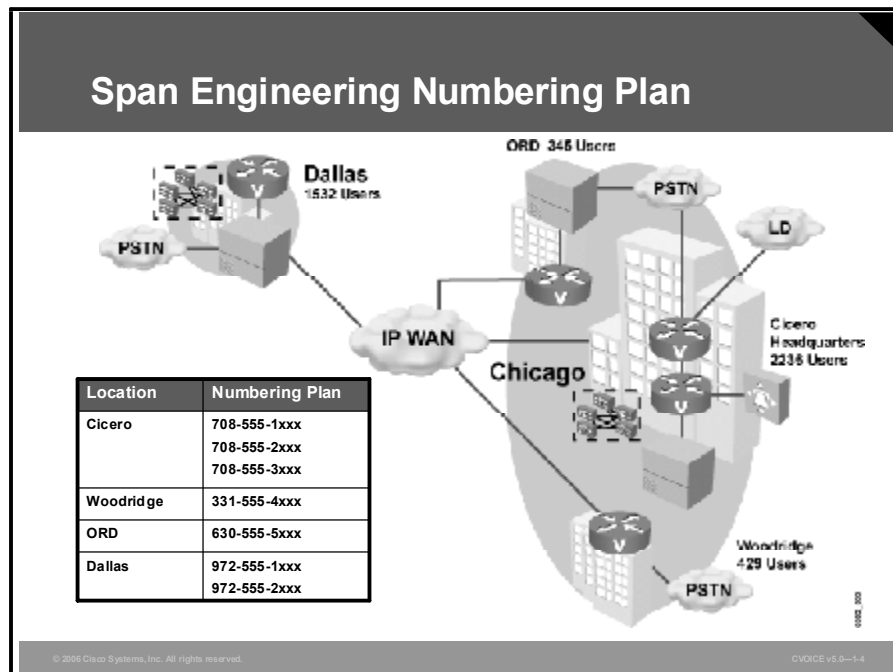
Implementing a VoIP network involves designing a numbering plan for all endpoints or reviewing an existing numbering plan for scalability and completeness. A dial plan can be designed only after the numbering plan has been completed and after call patterns and connectivity to the public switched telephone network (PSTN) are understood. All implementations of VoIP require both a numbering plan and a dial plan.

- **Numbering plan:** A numbering plan identifies each VoIP endpoint and application in the network with a unique telephone number. Numbering plan design should evaluate both current requirements and potential growth requirements to avoid the need to renumber as more users connect to the voice network. Types of numbering plans include the following:
 - **The international public telecommunication numbering plan (E.164):** The E.164 standard defines the use of a one-, two-, or three-digit country code, followed by the national destination code, followed by the subscriber number.
 - **National numbering plans:** A national numbering plan defines the numbering structure for a specific country or group of countries. An example is the North American Numbering Plan (NANP). It defines a 10-digit numbering plan. First is a three-digit Numbering Plan Area (NPA) commonly referred to as the area code. Next is a three-digit central office code. Finally there is a four-digit subscriber line number. The United States, Canada, and parts of the Caribbean, all use the NANP for number assignment. Other countries have differing national numbering plans. Familiarity with these plans is required when planning an international voice network.

- **Private numbering plans:** Private numbering plans are used to address endpoints and applications within private networks. Private numbering plans are not required to adhere to any specific format and can be created to accommodate the needs of the network. Because most private telephone networks connect to the PSTN at some point in the design, it is good practice to plan the private numbering plan to coincide with publicly assigned number ranges. Number translation may be required when connecting private voice networks to the PSTN.
- **Dial plans:** The dial plan is a key element of an IP telephony system and an integral part of all call-processing agents. Generally, the dial plan is responsible for instructing the call-processing agent on how to route calls. Specifically, the dial plan performs these main functions:
 - **Endpoint addressing:** Reachability of internal destinations is provided by assigning directory numbers to all endpoints (such as IP Phones, fax machines, and analog phones) and applications (such as voice-mail systems, auto attendants, and conferencing systems). Directory number assignment is based on the implemented numbering plan.
 - **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:** Different groups of devices can be assigned to different classes of service by 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.
 - **Digit manipulation:** In some cases, it is necessary to manipulate the dialed string before routing the call; for example, when rerouting over the PSTN a call that was originally dialed using the on-net access code. Another example is when 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. These might include top-down, circular hunt, longest idle, or broadcast.
 - **Overlapping number processing:** In some cases, administrators are tasked with connecting two or more voice networks with overlapping number ranges. For example, when two companies merge, company X may have a user number range of 1xxx, and company Y may also use the number range of 1xxx. When dealing with overlapping number ranges, one solution is to assign a unique site access code to each individual location. Users would then dial the access code, followed by the extension number. The number of digits used for the access code would depend on the total number of locations affected.

Example 1: Span Engineering Numbering Plan

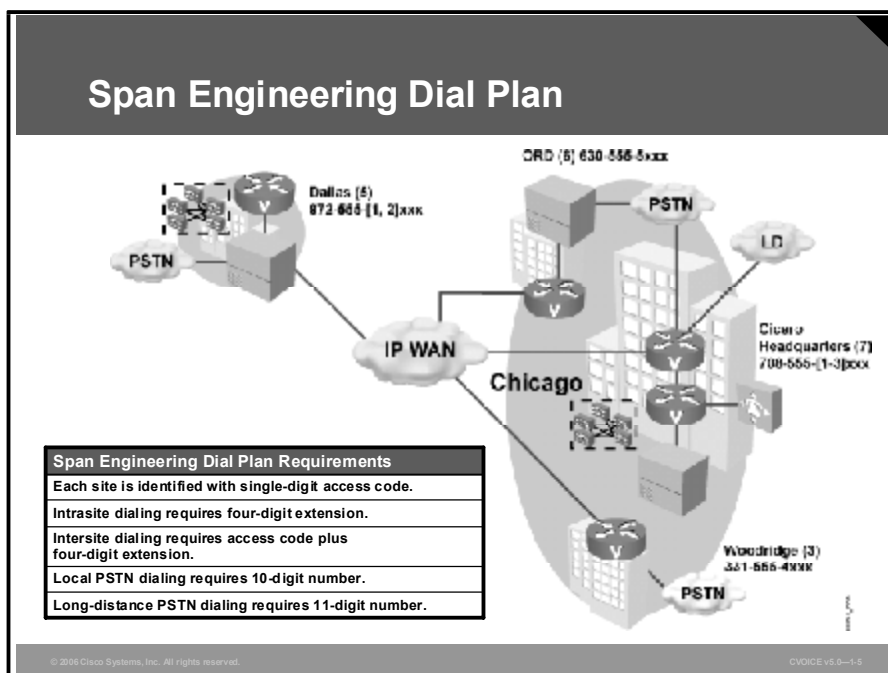
The figure shows the numbering plan for Span Engineering.



Span Engineering has multiple locations and is currently evaluating the numbering plan associated with its Chicago campuses and the Dallas location. The numbering plan design process includes enumerating the number of current users at each location and evaluating future growth requirements. The internal numbering plan will use the PSTN-assigned direct inward dialing (DID) numbers that have been allocated at each site.

Example 2: Span Engineering Dial Plan

The figure shows requirements for the Span Engineering dial plan.

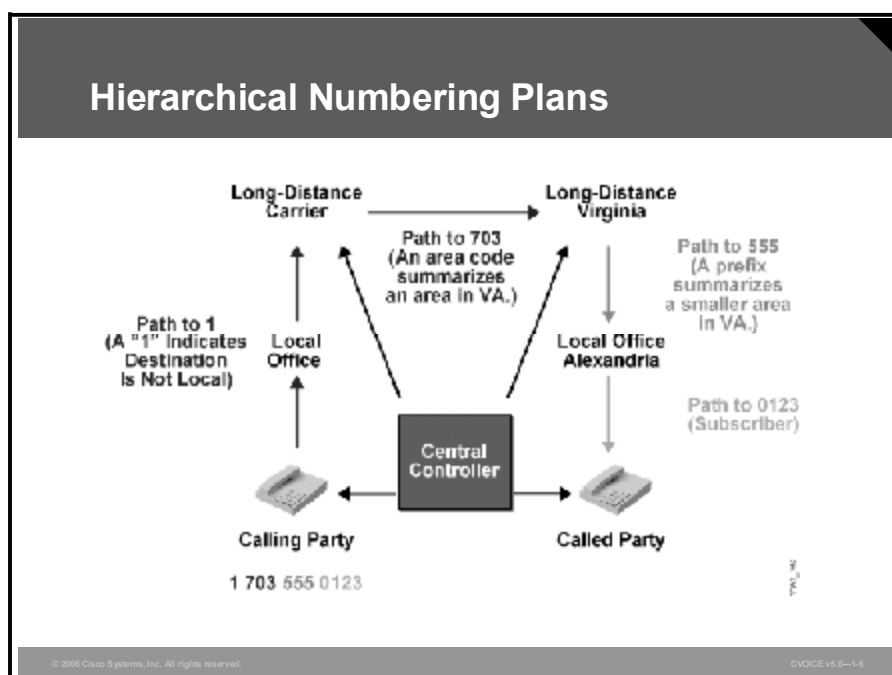


Here are the Span Engineering dial plan requirements:

- Single-digit (1–8) access code identifying each campus
- Single-digit (9) access code that directs calls to the local PSTN
- Intrasite dialing that is based on the four-digit extension
- Intersite dialing that is based on the access code plus the four-digit extension
- Local PSTN access that requires the access code 9 followed by the 10-digit number and also that the 9 is stripped and 10 digits are passed to the PSTN switch
- Long-distance PSTN access that requires the access code 9 followed by the digit 1, followed by the 10-digit number and also that the 9 is stripped and 11 digits are passed to the PSTN switch

Hierarchical Numbering Plans

This topic describes the advantages and attributes of hierarchical numbering plans.



Scalable telephony networks require telephone numbering plans that are hierarchical. A hierarchical design has these advantages:

- **Simplified provisioning:** Refers to the ability to easily add new groups and modify existing groups
- **Simplified routing:** Keeps local calls local and uses a specialized number key, such as an area code, for long-distance calls
- **Summarization:** Establishes groups of numbers in a specific geographical area or functional group
- **Scalability:** Provides additional high-level number groups
- **Management:** Controls number groups from a single point in the overall network

It is not easy to design a hierarchical numbering plan. Existing numbering plans in the network may include proprietary PBXs, key systems, and telephony services such as Centrex. The necessity to conform to the PSTN at the gateways will also contribute to the complexity of the design. Translation between these systems is a difficult task. If possible, avoid retraining system users. The goal is to design a numbering plan that has these attributes:

- Minimal impact on existing systems
- Minimal impact on users of the system
- Minimal translation configuration
- Consideration of anticipated growth

Example: Span Engineering Hierarchical Numbering Plan

Span Engineering will use the full 10-digit DID numbers that are assigned by the PSTN for the internal numbering plan of the company. Using the 10-digit numbers provides Span Engineering with these benefits:

- Allows easy integration to the PSTN at each local campus with minimal digit manipulation
- Allows dial plans to summarize call routing for sites that use multiple number ranges
- Provides flexibility for the dial plan to use shorter dialing patterns as extensions within the voice network

Internal Numbering and Public Numbering Plan Integration

This topic describes the challenges associated with integrating internal numbering with the public numbering plan.

Challenges Associated with Integration

- **Varying number lengths**
- **Specialized services**
- **Voice mail**
- **Necessity of prefixes or area codes**
- **International dialing consideration**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0—1.7

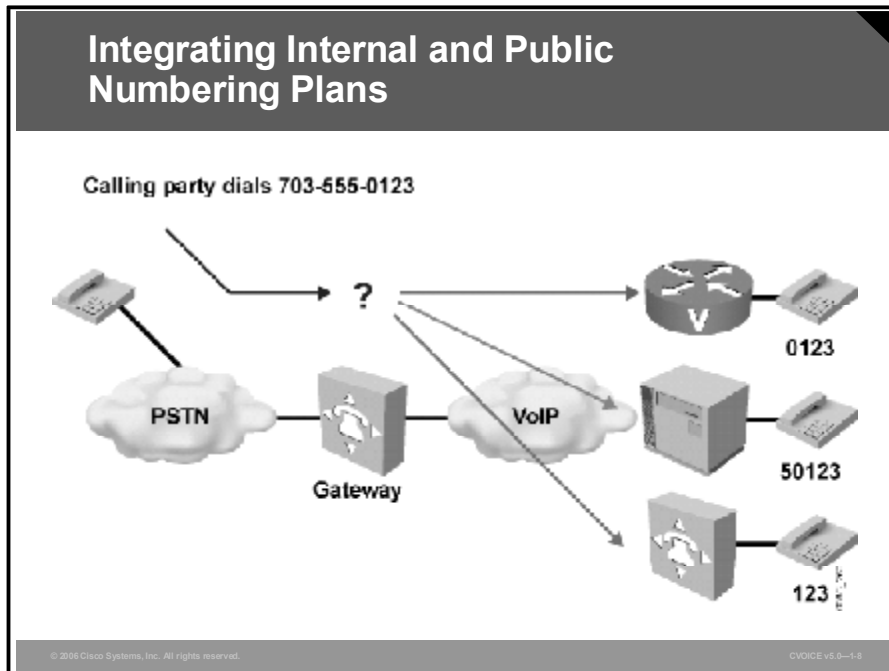
Numbering plans vary greatly throughout the world. Different countries use different number lengths and hierarchical plans within their borders. Telephony equipment manufacturers and service providers use nonstandard numbering. In an attempt to standardize numbering plans, the ITU developed the E.164 worldwide prefix scheme.

Numbering plan integration from an internal system such as a VoIP and PBX system to the PSTN requires careful planning. The hierarchical structure of the numbering plan and the problems associated with varying number lengths in different systems make numbering plan integration complex.

Here are some of the challenges that you face with numbering plan integration:

- **Varying number lengths:** Within the IP network, consideration is given to varying number lengths that exist outside the IP network. Local, long-distance, key system, and Centrex dialing from within the IP network may require digit manipulation.
- **Specialized services:** Services such as Centrex and their equivalents typically have four-digit or five-digit numbers. Dialing from the PSTN into a private VoIP network and then out to a Centrex extension can also require extensive digit manipulation.
- **Voice mail:** When a called party cannot be reached, the network may have to redirect the call to voice mail. Because the voice-mail system can require a completely different numbering plan than the endpoint telephones, translation is necessary.

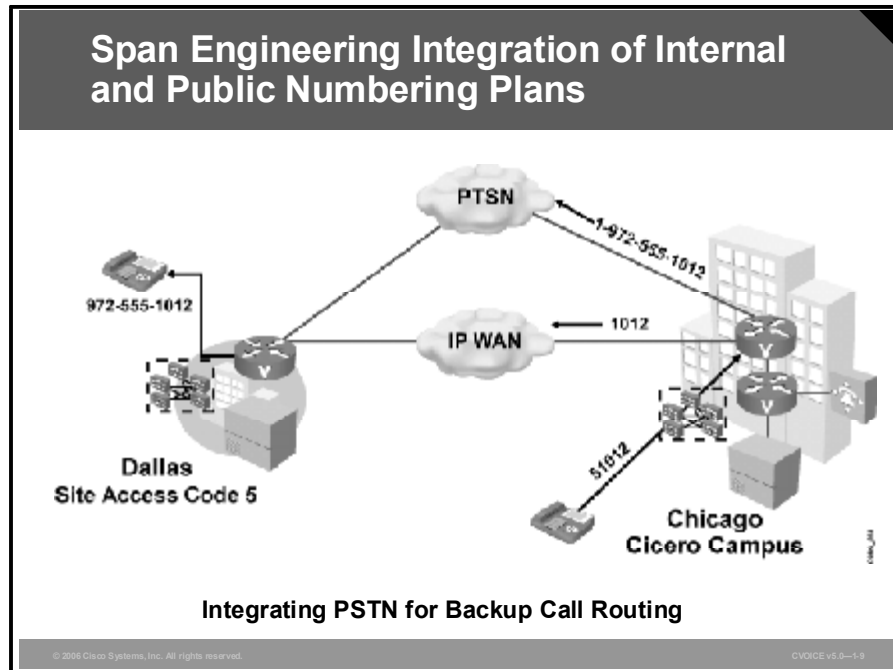
- **Necessity of prefixes or area codes:** It can be necessary to strip or add area codes, or prepend or replace prefixes. Rerouting calls from the IP network to the PSTN for failure recovery can require extra digits.
- **International dialing consideration:** Country codes and numbering plans vary in length within countries. Dialing through an IP network to another country requires careful consideration.



This figure shows a call from the PSTN destined for 1-703-555-0123. The gateway must realize the true destination. All endpoints conclude with the same digit sequence, but which is the correct endpoint? Should the gateway append or prepend digits to the dialed number? Should it strip and omit digits?

Example: Span Engineering Integration of Internal and Public Numbering Plans

This figure shows how Span Engineering integrates its internal numbering plan with the external public numbering plan.

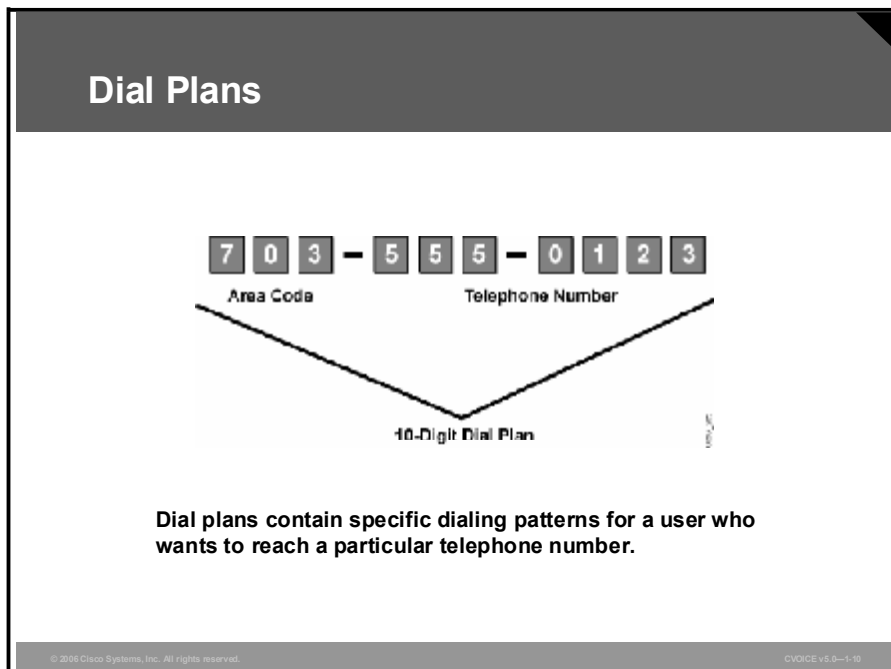


In this example, Span Engineering uses the PSTN as a backup route for calls between Cicero and Dallas.

- Step 1** The Cicero caller dials the site access code for Dallas (5) followed by the four-digit extension number of the destination phone (1012).
- Step 2** The voice gateway determines if the call can be completed using the IP WAN or if the call must be routed via the PSTN.
- Step 3** Digit manipulation occurs based on the path chosen.
 - Strip the site access code and send four digits if completing the call across the IP WAN.
 - Strip the site access code and prepend 1-972 if completing the call across the PSTN.

Scalable Dial Plans

This topic describes the need for a scalable dial plan in a VoIP network.



Although most people are not acquainted with dial plans by name, they use them daily.

Example: Dial Plan Implementations

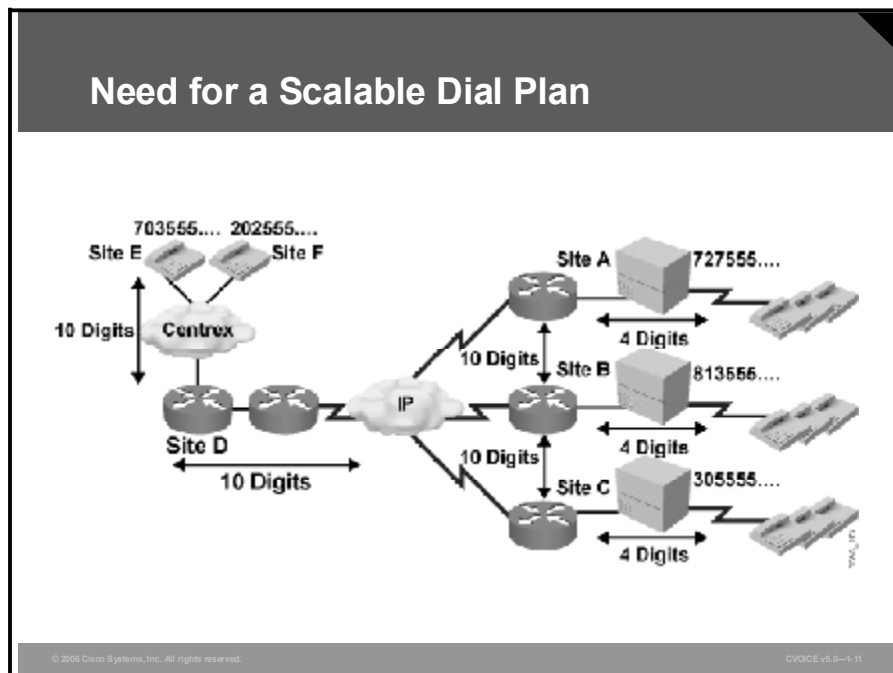
The North American telephone network is designed around a 10-digit numbering plan that consists of 3-digit area codes and 7-digit telephone numbers. For telephone numbers that are located within an area code, the PSTN uses a seven-digit dial plan. Features within a central office-based (CO-based) PBX, such as Centrex, allow the use of a custom five-digit dial plan for customers who subscribe to that service. PBXs are more flexible and allow for variable-length dial plans containing 3 to 11 digits.

Dial plans contain specific dialing patterns for a user who wants to reach a particular telephone number. Dial plans also contain access codes, area codes, specialized codes, and combinations of the numbers of digits dialed.

Dial plans require knowledge of the customer network topology, current telephone number dialing patterns, proposed router and gateway locations, and traffic-routing requirements. If the dial plans are for a private internal voice network that is not accessed by the outside voice network, the telephone numbers can be any number of digits.

Typically, companies that implement VoIP networks carry voice traffic within the least expensive systems and paths. Implementing this type of system involves routing calls through IP networks, private trunks, PBXs, key systems, and the PSTN. The numbering plan to support the system is scalable, easily understood by the user, and transportable between all of the system components. The use of alternate path components reduces instances of call failure. Finally, the numbering plan conforms to all applicable standards and formats for all of the systems involved.

Need for a Scalable Dial Plan



This figure illustrates a complex voice network that consists of the components discussed in this topic. A comprehensive and scalable dial plan must be well-planned and well-implemented on networks such as this. The Centrex service requires 10-digit dialing between itself and site D. The IP network requires 10-digit dialing toward sites A, B, and C. Each of the PBXs requires four-digit dialing.

Practice Item 1: Span Engineering Dial Plan Worksheet

Here is a list of specifications for the Span Engineering dial plan:

- The Cicero campus number ranges are 708-555-1xxx, 708-555-2xxx, and 708-555-3xxx.
- The Cicero Campus site access code is 7.
- The Dallas campus number ranges are 972-555-1xxx and 972-555-2xxx.
- The Dallas campus site access code is 5.
- The ORD (Span Engineering Chicago airport location) number range is 630-555-5xxx.
- The ORD site access code is 6.
- The PSTN requires digit dialing for local calls.
- The PSTN requires a “1” + 10 digits for long-distance calls.
- Cicero to ORD is local through PSTN.
- Cicero to Dallas is long distance through PSTN.
- Intrasite calls require a four-digit extension.
- Intersite calls require an access code and a four-digit extension.

Based on the dial plan worksheet, fill in the appropriate information in each space in the table. The first row has been filled in for you as an example.

Span Engineering Dial Plan

Call Information	Number Dialed	Number Sent to Remote Gateway Through WAN	Number Sent to PSTN
Cicero caller calls Dallas extension 2312	52312	2312	1-972-555-2312
Cicero caller calls ORD extension 5087			
Dallas caller calls Cicero extension 3312			
Dallas caller calls Dallas extension 2887			

Practice Item 1 Answer Key

Call Information	Number Dialed	Number Sent to Remote Gateway Through WAN	Number Sent to PSTN
Cicero caller calls Dallas extension 2312	52312	2312	1-972-555-2312
Cicero caller calls ORD extension 5087	65087	5087	630-555-5087
Dallas caller calls Cicero extension 3312	73312	3312	1-708-555-3312
Dallas caller calls Dallas extension 2887	2887	N/A	972-555-2887

Scalable Dial Plan Attributes

This topic describes the attributes of a scalable dial plan.

Attributes of a Scalable Dial Plan

- **Logic distribution**
- **Hierarchical design**
- **Simplicity in provisioning**
- **Reduction in postdial delay**
- **Availability and fault tolerance**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-12

When designing a large-scale dial plan, you must adhere to these attributes:

- **Logic distribution:** Good dial plan architecture relies on the effective distribution of the dial plan logic among the various components. Devices that are isolated to a specific portion of the dial plan reduce the complexity of the configuration. Each component focuses on a specific task accomplishment. Generally, the local switch or gateway handles details that are specific to the local point of presence (POP). Higher-level routing decisions are passed along to the gatekeepers and PBXs. A well-designed network places the majority of the dial plan logic at the gatekeeper devices.
- **Hierarchical design (scalability):** You must strive to keep the majority of the dial plan logic (routing decisions and failover) at the highest-component level. Maintaining a hierarchical design makes the addition and deletion of number groups more manageable. Scaling the overall network is much easier when configuration changes are made to a single component.
- **Simplicity in provisioning:** Keep the dial plan simple and symmetrical when designing a network. Try to keep consistent dial plans on the network by using translation rules to manipulate the local digit dialing patterns. These number patterns are normalized into a standard format or pattern before the digits enter the VoIP core. Putting digits into a standard format simplifies provisioning and dial-peer management.

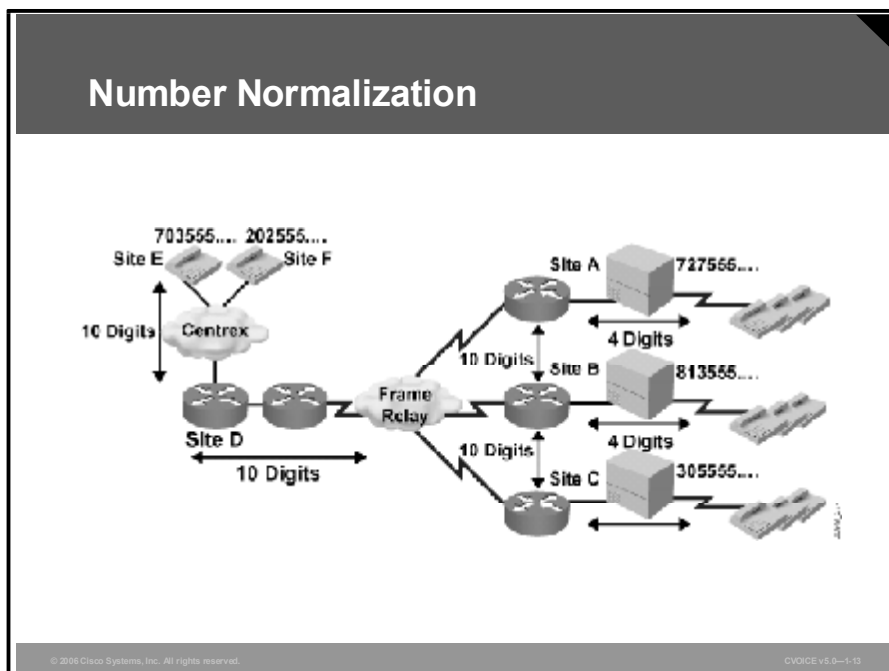
- **Reduction in postdial delay:** Consider the effects of postdial delay in the network when you design a large-scale dial plan. Postdial delay is the time between the last digit dialed and the moment the phone rings at the receiving location. In the PSTN, people expect a short postdial delay and to hear ringback within seconds. The more translations and lookups that take place, the longer the postdial delay becomes. Overall network design, translation rules, and alternate pathing affect postdial delay. You must strive to use these tools most efficiently to reduce postdial delay.
- **Availability and fault tolerance:** Consider overall network availability and the call success rate when you design a dial plan. Fault tolerance and redundancy within VoIP networks are most important at the gatekeeper level. By using an alternate path, you help provide redundancy and fault tolerance in the network.
- **Conformance to public standards, where applicable**

Example: Span Engineering Dial Plan Attributes

To provide a robust and scalable VoIP network environment, Span Engineering is configuring backup call routes through each local PSTN access. Digit manipulation required for PSTN access is configured at the local PSTN gateway device. Call Admission Control (CAC) and call routing are configured in Cisco CallManager. By assigning the dial plan the same DID numbers as are assigned by the service provider, the administrator has a consistent picture of what type of digit manipulation is required to reach any number that is dialed.

Enhancing and Extending an Existing Numbering Plan to Accommodate VoIP

This topic describes methods for integrating existing numbering plans into a VoIP network.



There are many ways that you can enhance and extend an existing numbering plan to accommodate the VoIP network; all of them require careful planning and consideration. This lesson will discuss two of these ways: number normalization and technology prefixes.

Example: Number Normalization

When site E (703555...) dials 7275550199, the full 10-digit dialed string is passed through the Centrex to the router at site D. Router D matches the destination pattern 7275550199 and forwards the 10-digit dial string to router A. Router A matches the destination pattern 727555..., strips off the matching 727555, and forwards the remaining four-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. However, because the Centrex service requires the full 10-digit dial string to complete calls, the plain old telephone service (POTS) dial peer at router D is configured with digit stripping disabled. An alternate solution involves enabling digit stripping and configuring the dial peer with a six-digit prefix (in this case, 703555), which results in forwarding the full dial string to the Centrex service.

Router Digit Stripping Comparison

Router A	Router D
dial-peer voice 1 pots	dial-peer voice 4 pots
destination-pattern 727555....	destination-pattern 703555....
port 1/0:1	no digit-strip
!	port 1/0:1
dial-peer voice 4 voip	!
destination-pattern 703555....	dial-peer voice 5 pots
session target ipv4:10.10.10.2	destination-pattern 202555....
!	no digit-strip
dial-peer voice 5 voip	port 1/0:1
destination-pattern 202555....	!
session target ipv4:10.10.10.3	dial-peer voice 1 voip
!	destination-pattern 727555....
	session target ipv4:10.10.10.1
	!

Another method, called technology prefixes, allows you to include special characters in the called number. These special characters (most commonly designated as 1#, 2#, 3#, etc.) are prepended to the called number on the outgoing VoIP dial peer. The gatekeeper then checks its gateway technology prefix table for gateways that are registered with that particular technology prefix. Technology prefixes also identify a type of gateway, a class of gateway, or a pool of gateways.

Example: Technology Prefixes Applied

Voice gateways can register with technology prefix 1#; H.320 gateways with technology prefix 2#; and voice-mail gateways with technology prefix 3#. Multiple gateways can register with the same type prefix. When this happens, the gatekeeper makes a random selection among gateways of the same type.

If the callers know the type of device that they are trying to reach, they can include the technology prefix in the destination address to indicate the type of gateway to use to get to the destination. For example, if a caller knows that address 7275550111 belongs to a regular telephone, the caller can use the destination address of 1#7275550111, where 1# indicates that the address should be resolved by a voice gateway. When the voice gateway receives the call for 1#7275550111, it strips off the technology prefix and routes the next leg of the call to the telephone at 7275550111.

You can enter technology prefix commands on gateways and gatekeepers in two places, depending on how you want to design the technology prefix decision intelligence: the gateway VoIP interface or the gateway dial peer.

You can implement this type of digit manipulation and management of dialed numbers in various ways, depending on the infrastructure of the network. All of the components, including

the gatekeepers, gateways, Cisco CallManagers, PBXs, key systems, and other systems, may need to be included in the process.

Accounting for Caller Mobility for 911 Services

This topic describes how VoIP operators can provide the location and telephone number of mobile callers to 911 operators.

911 Terms and Components

- **ANI: The calling party number**
- **ALI: A database record of telephone number-to-geographic location association; typically located in the PSTN**
- **PSAP: Normally a police or sheriff-run call center**
- **ERL: The area from which an emergency call is placed and to which a 911 Emergency Response Team (ERT) may be dispatched; used in VoIP mobility environments**
- **ELIN: A phone number that is used to route the emergency call to the local PSAP, and which the PSAP can use to call back the emergency caller; used in VoIP mobility environments**
- **MSAG: Maintained by a government agency; lists which PSAP serves a particular address range**
- **Selective router: A specialized telephone switch used for 911 that routes calls to the appropriate PSAP based on calling number (ANI) instead of called number**
- **CAMA: An analog phone trunk that connects directly to an 911 selective router, bypassing the PSTN**
- **Cisco Emergency Responder: A Cisco application used in a mobile VoIP environment to automatically track and update equipment moves and changes**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v9.0-1-14

To understand how VoIP operators can provide the location and telephone number for 911 services, you must understand the function of the basic components. The basic components of 911 services are as follows:

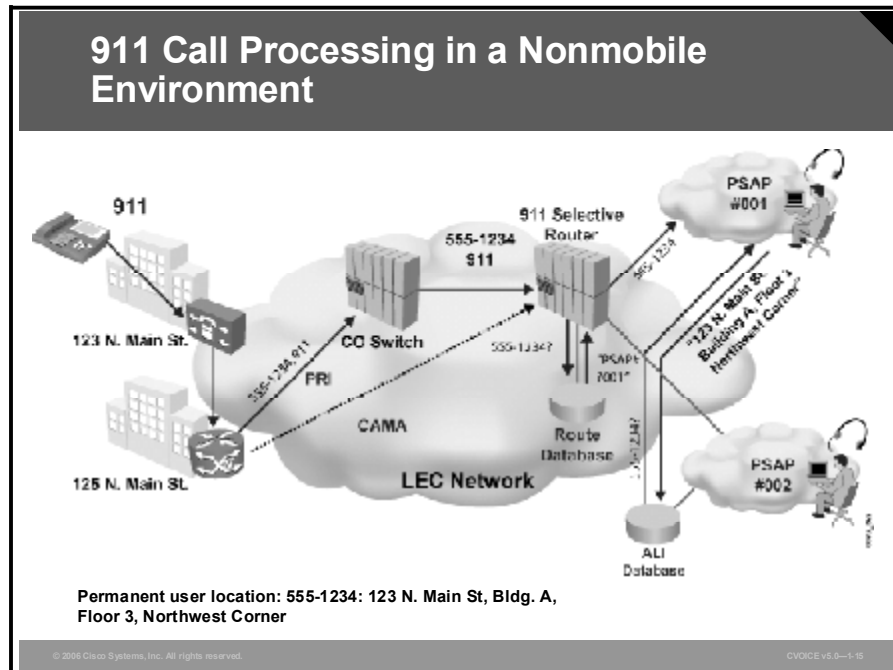
- **Automatic number identification (ANI):** ANI is the calling-party number that is included with each call to identify where the call originated. Often, in a business environment, the original ANI may be changed by the service provider at the first switch to reflect the billing number of the company instead of reflecting the calling number of the original party. Discussions with the service provider need to ensure that the original ANI is transmitted with all calls. Internal extensions or private numbering plans require mapping or translation for outbound ANI.
- **Automatic location identification (ALI):** The ALI database contains the records that map telephone numbers to geographic locations. The ALI database resides in the service provider network. Updates to the ALI database are submitted any time that there is a move, add, or change event in a telephony network. Updates can take up to 48 hours to take effect, thereby making dynamic ALI updates unsuitable in a mobile environment.
- **Public safety answering point (PSAP):** The PSAP is the answer point where the emergency call is terminated. Calls are directed to specific PSAPs based on the geographic location of the call origination point.

- **Emergency response location (ERL):** ERL is the location from which an emergency call is placed. In a network where VoIP mobility is common, the ANI of the calling telephone does not always identify the location of the emergency, because the callers retain the same extension regardless of where they are actually located. The ERL is used in mobility environments by associating ports and devices to an ERL group. The recommendation is to define an ERL group for each floor in a building, each unit in a hotel or motel, or each tenant in a multitenant building.
- **Emergency location identification number (ELIN):** An ELIN is a NANP telephone number that is used for routing an emergency call to the appropriate PSAP. In a mobile environment where the ANI is the mobile extension of the user, the ELIN is substituted for the ANI when the call is sent to the PSAP. This substitution enables the PSAP to record the calling number and be able to call the number back if the need arises. Each ERL has a unique ELIN associated with it. When a mobile caller logs into the VoIP phone, the ELIN for the call is determined based on the ERL that the port is associated with.
- **Master street address guide (MSAG):** MSAG is a database that is maintained by a government agency. This database maps geographic locations to the PSAPs that are responsible for handling emergency calls for those locations.
- **Selective router:** A selective router is a dedicated 911 switch in the service provider network that routes 911 calls to the appropriate PSAP based on the calling number. This approach is different from normal call routing, which routes based on the called number. When a call is routed to the selective router, the router looks at the ANI and determines which PSAP to send the call to.
- **Centralized Automated Message Accounting (CAMA):** A CAMA is an analog trunk that connects a customer switch directly to the selective router in the service provider network. A CAMA trunk carries 911 calls only; it does not carry other user calls.
- **Cisco Emergency Responder:** Cisco Emergency Responder is an application that automatically tracks and updates moves and changes of equipment, thereby removing this burden from the administrative staff and providing cost savings. Through a real-time, location tracking database, the Cisco Emergency Responder also allows emergency personnel to identify locations of 911 callers. The Cisco Emergency Responder works in conjunction with Cisco CallManager.

It is critical that the network designer understand and adhere to local, municipal, state, and federal laws regarding compliance to 911 requirements.

Example: 911 Call Processing in a Nonmobile Environment

This example is based on an environment where telephony end devices remain in their permanent location.

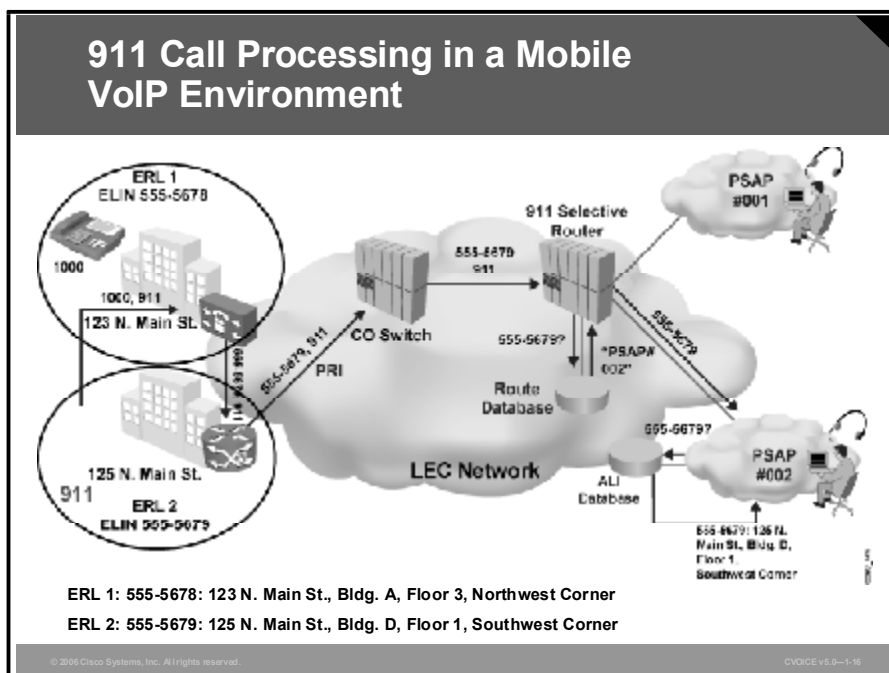


The call is processed as follows:

1. The emergency call originates from the device with the ANI of 555-1234.
2. The call is routed via Cisco CallManager to the main PSTN gateway at the headquarters.
3. The PSTN gateway either routes the call directly to the selective router via the CAMA trunk (if present) or routes the call via the normal PRI connection to the CO switch.
4. The CO switch retains the original ANI and does not replace it with the billing number.
5. The CO switch routes the call to the selective router.
6. The selective router queries the database to determine which PSAP is responsible for the location of the ANI.
7. The selective router routes the call to the PSAP.
8. The PSAP queries the ALI database to determine the exact location of the caller.

Example: 911 Call Processing in a Mobile Environment

Cisco Emergency Responder is used to dynamically update location information for mobile users. In this example, the user with extension 1000 is normally located at 123 N. Main Street but is working on a project with a team at the headquarters, which is located at 125 N. Main Street. The emergency call is placed by the user of extension 1000 at the 125 N. Main Street location.



The call is processed as follows:

1. The user with extension 1000 logs into a VoIP phone plugged into a switch that is configured for ERL 2.
2. The ERL 2 has ELIN 555-5679 associated with it.
3. The Cisco Emergency Responder queries Cisco CallManager to determine when new users log into a VoIP telephone. Cisco Emergency Responder queries Cisco Catalyst switches to determine the port that the user is plugged into.
4. The Cisco Emergency Responder determines the ELIN based on the ERL configuration for the port.
5. The Cisco Emergency Responder replaces the original ANI of 1000 with the ELIN of ERL 2 (which is 555-5679) and forwards the call to the gateway connected to the PSTN.
6. The CO switch routes the call to the selective router.
7. The selective router queries the database to determine which PSAP is responsible for the location of the ANI.
8. The selective router routes the call to the PSAP.
9. The PSAP queries the ALI database to determine the exact location of the caller.

Practice Item 2: Numbering Plan for Span Engineering

Chicago Airport Location

The Span Engineering Chicago airport location (referred to as ORD) uses the number range of 630-555-5000 through 630-555-5999. Before the start of migration to VoIP, all employees at ORD are connected to each other and to the PSTN through the local PBX. The first phase of migration consists of moving a small group of 10 users off the PBX and onto the VoIP infrastructure. The 10 users who are to be migrated use the extension range of 5100 through 5110. Define the new numbering ranges that will be used for connectivity to all staff at ORD.

ORD numbering range (or ranges) for PBX:

ORD numbering range (or ranges) for VoIP phones:

London Location

Span Engineering collaborates with several companies in London, England. The telephone number range to reach the London facilities is 7946 0300 through 7946 0350. The area code for London is 020 and the country code is 44. All calls that originate in the United States and are destined for international carriers must begin with the international access code of 011. This access code must be followed by the country code, area code, and local telephone number.

The internal code within Span Engineering for dialing London locations is “2” plus a four-digit extension, which is the last four digits of the telephone number. Define the requested dialing patterns for users located at ORD who are dialing the London offices, based on a call from ORD to London extension 0344.

Number dialed by ORD staff:

Number that needs to be sent to the PSTN to complete the overseas call:

Practice Item 2 Answer Key

Chicago Airport Location

ORD numbering ranges for PBX:

- 630-555-0000 through 630-555-5099
- 630-555-5111 through 630-555-5999

ORD numbering range for VoIP phones:

- 630-555-5100 through 630-555-5110

London Location

Number dialed by ORD staff:

- 20344

Number that needs to be sent to the PSTN to complete the overseas call:

- 0114402079460344

Summary

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

Summary

- **Numbering plans define telephone numbers for voice endpoints and applications, whereas dial plans define call routing and digit manipulation.**
- **Overlapping number ranges are addressed through the use of site access codes.**
- **The associated attributes of a hierarchical numbering plan are simplified provisioning and routing, summarization, scalability, and management. These attributes provide minimal system and configuration impact, anticipated growth consideration, and conformance to public standards, where applicable.**
- **Varying number lengths, specialized services, voice mail, necessity of prefixes or area codes, and international dialing considerations are challenges associated with integrating an internal numbering plan with the public numbering plan.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-1-17

Summary (Cont.)

- **Because implementing a scalable dial plan involves extensive call routing, it is important to understand a customer network topology, number dialing patterns, router and gateway locations, and traffic requirements.**
- **The required design-simplification attributes of a scalable numbering plan provide increased manageability and increased call service and delivery.**
- **Digit manipulation and the addition of technology prefixes are methods to extend and enhance VoIP numbering plans.**
- **Cisco Emergency Responder dynamically tracks the adds, moves, and changes of mobile VoIP users and replaces the ANI with the ELIN to identify the current location of the originator.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-1-18

References

For additional information, refer to these resources:

- *Designing a Static Dial Plan.*
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/dp3_isd.htm.
- *Understanding One Stage and Two Stage Voice Dialing.*
<http://www.cisco.com/warp/public/788/voip/1stage2stage.html>.
- *Voice Design and Implementation Guide.*
<http://www.cisco.com/warp/public/788/pkt-voice-general/8.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) Which function best describes a numbering plan?

- A) determines routes between source and destination
- B) defines a telephone number of a voice endpoint or application
- C) performs digit manipulation when sending calls to the PSTN
- D) performs least-cost routing for VoIP calls

Q2) Match each function of a dial plan with its description.

- A) endpoint addressing
 - B) path selection
 - C) calling privileges
 - D) digit manipulation
 - E) overlapping number range processing
- _____ 1. uses a unique site access code per location to resolve the problem
- _____ 2. determines which destinations are allowed to be accessed from each source
- _____ 3. translates, strips, or prepends digits to the dialing string that is being processed
- _____ 4. determines whether the primary path or secondary path should be used to process the call
- _____ 5. identifies an endpoint by using a directory number

Q3) Match the advantage of a hierarchical numbering plan with its definition.

- A) simplified provisioning
 - B) simplified routing
 - C) summarization
 - D) scalability
 - E) management
- _____ 1. adds more high-level number groups
- _____ 2. provides the ability to add new groups and modify existing groups easily
- _____ 3. controls number groups from a single point in the overall network
- _____ 4. establishes a group of numbers in a specific geographical area or functions group
- _____ 5. keeps local calls local and uses a specialized number key, such as an area code, for long-distance calls

- Q4) Which two factors make the design of hierarchical numbering plans complex?
(Choose two.)
- A) requirements of long-distance calls
 - B) varying number lengths
 - C) number of geographical areas to be included in the network
 - D) billing mechanisms
 - E) necessity of prefixes or area codes
- Q5) Which of the challenges associated with integration requires translations?
- A) varying number lengths
 - B) specialized services
 - C) voice mail
 - D) necessity of prefixes or area codes
 - E) international dialing
- Q6) Which worldwide prefix scheme was developed by the ITU to standardize numbering plans?
- A) G.114
 - B) E.164
 - C) G.164
 - D) E.114
- Q7) The North American Numbering Plan is based on how many digits?
- A) 3
 - B) 7
 - C) 10
 - D) 11
- Q8) Which three types of information do you need to design a dial plan for a customer?
(Choose three.)
- A) network topology
 - B) traffic-routing requirements
 - C) current dialing patterns
 - D) proposed router and gateway locations
 - E) type of PBX and PSTN connection
- Q9) Match the attribute of a scalable numbering plan with its description.
- A) logic distribution
 - B) hierarchical design
 - C) simplicity in provisioning
 - D) reduction in postdial delay
 - E) availability and fault tolerance
- _____ 1. uses alternate paths to make sure there is overall network availability and call success rates
 - _____ 2. makes the addition and deletion of number groups more manageable
 - _____ 3. gives the network components the ability to focus on specific tasks to complete calls
 - _____ 4. is affected by network design, translation rules, and alternate paths
 - _____ 5. keeps dial plans consistent on the network by using translation rules to manipulate the local digit dialing patterns

- Q10) When distributing the dial plan logic, the majority of the dial plan logic should be placed at the _____.
A) dial peers
B) edge devices
C) gatekeepers
D) gateways
- Q11) Choose two locations where you can enter technology prefix commands. (Choose two.)
A) PBXs
B) gatekeepers
C) gateways
D) key systems
E) selective routers
- Q12) Technology prefixes can be used to identify _____. (Choose three.)
A) type of gateway
B) class of gateway
C) pool of gateways
D) gatekeeper zone
E) gatekeeper class
F) gatekeeper location
- Q13) In a mobile VoIP environment, the Cisco Emergency Responder replaces the ANI with the _____ before sending the emergency call to the PSTN.
A) ERL
B) PSAP
C) ELIN
D) NANP
- Q14) Which function best describes the ALI?
A) a database that determines which PSAP services each geographic area.
B) an analog trunk that connects the gateway directly to the selective router and is used only for 911 calls
C) a database that associates a telephone number to a specific location description
D) a specialized telephony switch that routes calls based on the calling number as opposed to the called number

Lesson Self-Check Answer Key

- Q1) B
Relates to: Numbering and Dial Plans
- Q2) 1-E
2-C
3-D
4-B
5-A
Relates to: Numbering and Dial Plans
- Q3) 1-D
2-A
3-E
4-C
5-B
Relates to: Hierarchical Numbering Plans
- Q4) B, E
Relates to: Hierarchical Numbering Plans
- Q5) C
Relates to: Internal Numbering and Public Numbering Plan Integration
- Q6) B
Relates to: Internal Numbering and Public Numbering Plan Integration
- Q7) C
Relates to: Scalable Dial Plans
- Q8) A, B, C
Relates to: Scalable Dial Plans
- Q9) 1-E
2-B
3-A
4-D
5-C
Relates to: Scalable Dial Plan Attributes
- Q10) C
Relates to: Scalable Dial Plan Attributes
- Q11) B, C
Relates to: Enhancing and Extending an Existing Numbering Plan to Accommodate VoIP
- Q12) A, B, C
Relates to: Enhancing and Extending an Existing Numbering Plan to Accommodate VoIP
- Q13) C
Relates to: Accounting for Caller Mobility for 911 Services
- Q14) C
Relates to: Accounting for Caller Mobility for 911 Services

Lesson 4

Calculating Bandwidth Requirements

Overview

This lesson describes, in detail, the bandwidth requirements for Voice over IP (VoIP). Several variables affecting total bandwidth are explained, as well as the method of calculating and reducing total bandwidth.

Relevance

Because WAN bandwidth is probably the most expensive component of an enterprise network, network administrators must know how to calculate the total bandwidth required for voice traffic and how to reduce overall consumption.

Objectives

Upon completing this lesson, you will be able to list the bandwidth requirements for various coder-decoder (codecs) and data links, and describe the methods to reduce bandwidth consumption. This ability includes being able to meet these objectives:

- List five types of codecs and their associated bandwidth requirements
- Describe how the number of voice samples that are encapsulated impacts bandwidth requirements
- List the overhead for various Layer 2 protocols
- Describe how IPSec and GRE/L2TP affect bandwidth overhead
- Use a formula to calculate the total bandwidth that is required for a VoIP call
- Describe the operation of, and bandwidth savings associated with, the use of VAD

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Basic knowledge of VoIP
- Basic knowledge of TCP/IP networks
- Basic knowledge of Layer 2 technologies such as Frame Relay and ATM
- Basic knowledge of voice compression standards

Outline

The outline lists the topics included in this lesson.

Outline

- **Overview**
- **Codec Bandwidths**
- **Impact of Voice Samples and Packet Size on Bandwidth**
- **Data Link Overhead**
- **Security and Tunneling Overhead**
- **Calculating the Total Bandwidth for a VoIP Call**
- **Effects of VAD on Bandwidth**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-1-2

Codec Bandwidths

This topic describes the bandwidth that each codec uses and illustrates its impact on total bandwidth.

Bandwidth Implications of Codec								
Codec	G.711	G.726 r32	G.726 r24	G.726 r16	G.728	G.729	G.723 r63	G.723 r53
Bandwidth	64 kbps	32 kbps	24 kbps	16 kbps	16 kbps	8 kbps	6.3 kbps	5.3 kbps

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v9.0-1-3

One of the most important factors for the network administrator to consider while building voice networks is proper capacity planning. Network administrators must understand how much bandwidth is used for each VoIP call. With a thorough understanding of VoIP bandwidth, the network administrator can apply capacity planning tools.

Here is a list of codecs and their associated bandwidth:

- **G.711:** The G.711 pulse code modulation (PCM) coding scheme uses the most bandwidth. The G.711 PCM coding scheme takes samples 8000 times per second, each of which is 8 bits in length, for a total of 64,000 bps.
- **G.726:** The G.726 adaptive differential pulse code modulation (ADPCM) coding schemes use somewhat less bandwidth. While each coding scheme takes samples 8000 times per second like PCM, G.726 uses 4, 3, or 2 bits for each sample, thereby resulting in total bandwidths of 32,000 bps, 24,000 bps, or 16,000 bps.
- **G.728:** The G.728 low-delay code excited linear prediction (LDCELP) coding scheme compresses PCM samples using codebook technology. The G.728 LDCELP coding scheme uses a total bandwidth of 16,000 bps.
- **G.729:** The G.729 and G.729 Annex A (G.729A) Conjugate Structure Algebraic Code Excited Linear Prediction (CS-ACELP) coding scheme also compresses PCM using advanced codebook technology. This coding scheme uses 8000 bps total bandwidth.
- **G.723:** The G.723 and G.723 Annex A (G.723A) multipulse maximum likelihood quantization (MPMLQ) coding schemes use a look-ahead algorithm. These compression schemes result in 6300 bps or 5300 bps.

The network administrator should balance the need for voice quality against the cost of bandwidth in the network when choosing codecs. The higher the codec bandwidth is, the higher the cost of each call across the network will be.

Impact of Voice Samples and Packet Size on Bandwidth

This topic illustrates the effect of voice sample size on bandwidth.

Impact of Voice Samples			
Codec	Bandwidth	Sample Size	Packets
G.711	64,000	240	33
G.711	64,000	160	60
G.726r32	32,000	120	33
G.726r32	32,000	80	60
G.726r24	24,000	80	25
G.726r24	24,000	60	33
G.726r16	16,000	80	25
G.726r16	16,000	40	60
G.728	16,000	80	13
G.720	16,000	40	25
G.729	8000	40	25
G.729	8000	20	60
G.723r53	5300	40	17
G.723r53	5300	24	33
G.723r53	5300	40	17
G.723r53	5300	20	33

Voice sample size is a variable that can affect the total bandwidth used. A voice sample is defined as the digital output from a codec digital signal processor (DSP) that is encapsulated into a protocol data unit (PDU). Cisco uses DSPs that samples output based on digitization of 10 ms-worth of audio. Cisco voice equipment encapsulates 20 ms of audio in each PDU by default, regardless of the codec used. You can apply an optional configuration command to the dial peer to vary the number of samples encapsulated. When you encapsulate more samples per PDU, total bandwidth is reduced. However, encapsulating more samples per PDU comes at the risk of larger PDUs, which can cause variable delay and severe gaps if PDUs are dropped.

Example: Encapsulated Bytes Calculation

Using a simple formula, it is possible for you to determine the number of bytes encapsulated in a PDU based on the codec bandwidth and the sample size (20 ms is default), as follows:

$$\text{Bytes_per_Sample} = (\text{Sample_Size} * \text{Codec_Bandwidth}) / 8$$

If you apply G.711 numbers, the formula reveals the following:

$$\text{Bytes_per_Sample} = (0.020 * 64,000) / 8$$

$$\text{Bytes_per_Sample} = 160$$

The figure illustrates various codecs and sample sizes and the number of packets that are required for VoIP to transmit one second of audio. The larger the sample size, the larger the packet, and the fewer the encapsulated samples that have to be sent (which reduces bandwidth).

Data-Link Overhead

This topic lists overhead sizes for various Layer 2 protocols.

Data-Link Overhead

- **Ethernet II**
 - 18 bytes of overhead
- **MLP**
 - 6 bytes of overhead
- **Frame Relay**
 - 6 bytes of overhead

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-5

Another contributing factor to bandwidth is the Layer 2 protocol used to transport VoIP. VoIP alone carries a 40-byte IP/User Datagram Protocol (UDP)/Real-Time Transport Protocol (RTP) header, assuming uncompressed RTP. Depending on the Layer 2 protocol used, the overhead could grow substantially. The larger the Layer 2 overhead, the more bandwidth required to transport VoIP. These points illustrate the Layer 2 overhead for various protocols:

- **Ethernet II:** Carries 18 bytes of overhead; 6 bytes for source MAC, 6 bytes for destination MAC, 2 bytes for type, and 4 bytes for cyclic redundancy check (CRC)
- **Multilink Point-to-Point Protocol (MLP):** Carries 6 bytes of overhead; 1 byte for flag, 1 byte for address, 2 bytes for control (or type), and 2 bytes for CRC
- **Frame Relay Forum Standard 12 (FRF.12):** Carries 6 bytes of overhead; 2 bytes for data-link connection identifier (DLCI) header, 2 bytes for FRF.12, and 2 bytes for CRC

Security and Tunneling Overhead

This topic describes the overhead associated with various security and tunneling protocols.

Security and Tunneling Overhead

- **IPSec**
 - **50 to 57 bytes**
- **L2TP/GRE**
 - **24 bytes**
- **MLPPP**
 - **6 bytes**
- **MPLS**
 - **4 bytes**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0-1-8

Certain security and tunneling encapsulations will also add overhead to voice packets and should be considered when calculating bandwidth requirements. When using a Virtual Private Network (VPN), IP Security (IPSec) will add 50 to 57 bytes of overhead, a significant amount when considering small voice packets. Layer 2 Tunneling Protocol/generic routing encapsulation (L2TP/GRE) adds 24 bytes. When using MLP, 6 bytes will be added to each packet. Multiprotocol Label Switching (MPLS) adds a 4-byte label to every packet. All these specialized tunneling and security protocols must be considered when planning for bandwidth demands.

Example: VPN Overhead

Many companies have their employees telecommute from home. These employees initiate a VPN connection into their enterprise for secure Internet transmission. When deploying a remote telephone at the home of an employee using a router and a PBX Off-Premises eXtension (OPX), the voice packets will experience additional overhead associated with the VPN.

Calculating the Total Bandwidth for a VoIP Call

This topic calculates the total bandwidth required for a VoIP call using codec, data link, and sample size.

Total Bandwidth Required					
Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with CRTP	Ethernet
	Bits per Second	Bytes	Bits per Second	Bits per Second	Bits per Second
G.711	64,000	240	76,267	66,133	79,467
G.711	64,000	160	82,400	67,200	87,200
G.726r32	32,000	120	44,267	34,133	47,467
G.726r32	32,000	80	50,400	35,200	55,200
G.726r24	24,000	80	37,800	26,400	41,400
G.726r24	24,000	60	42,400	27,200	47,200
G.726r16	16,000	80	25,200	17,600	27,600
G.726r16	16,000	40	34,400	19,200	39,200
G.728	16,000	80	25,200	17,600	27,600
G.728	16,000	40	34,400	19,200	39,200
G.729	8000	40	17,200	9600	19,600
G.729	8000	20	26,400	11,200	31,200
G.723r63	6300	48	12,338	7350	13,913
G.723r63	6300	24	18,375	8400	21,525
G.723r53	5300	40	11,395	6360	12,985
G.723r53	5300	20	17,490	7420	20,670

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-7

Codec choice, data-link overhead, sample size, and compressed RTP have positive and negative impacts on total bandwidth. To perform the calculations, you must consider these contributing factors as part of the equation:

- More bandwidth required for the codec = more total bandwidth required
- More overhead associated with the data link = more total bandwidth required
- Larger sample size = less total bandwidth required
- Compressed RTP = significantly reduced total bandwidth required

Example: Total Bandwidth Calculation for Span Engineering

Span Engineering is implementing VoIP to carry voice calls between all sites. WAN connections between sites will carry both data and voice. To use bandwidth efficiently and keep costs to a minimum, voice traffic traversing the WAN will be compressed using the G.729 codec with 20-byte voice samples. WAN connectivity will be through a Frame Relay provider.

The following calculation was used to calculate total bandwidth per call:

$$\text{Total_Bandwidth} = ([\text{Layer_2_Overhead} + \text{IP_UDP_RTP Overhead} + \text{Sample_Size}] / \text{Sample_Size}) * \text{Codec_Speed}$$

The calculation for the G.729 codec, 20-byte sample size, using Frame Relay *without* Compressed RTP (CRTP) is as follows:

$$\text{Total_Bandwidth} = ([6 + 40 + 20] / 20) * 8000$$

$$\text{Total_Bandwidth} = 26,400 \text{ bps}$$

The calculation for the G.729 codec, 20-byte sample size, using Frame Relay *with* CRTP is as follows:

$$\text{Total_Bandwidth} = ([6 + 2 + 20] / 20) * 8000$$

$$\text{Total_Bandwidth} = 11,200 \text{ bps}$$

Effects of VAD on Bandwidth

This topic describes the effect of voice activity detection (VAD) on total bandwidth.

Effect of VAD

Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with VAD
G.711	64,000	240	76,267	49,573
G.711	64,000	160	82,400	53,560
G.726r32	32,000	120	44,267	28,773
G.726r32	32,000	80	60,400	32,760
G.726r24	24,000	80	37,800	24,570
G.726r24	24,000	80	42,400	27,560
G.726r16	16,000	80	25,200	16,380
G.726r16	16,000	40	34,400	22,360
G.728	16,000	80	25,200	16,380
G.728	16,000	40	34,400	22,360
G.729	8000	40	17,200	11,180
G.729	8000	20	26,400	17,180
G.723r63	6300	40	12,338	8019
G.723r63	6300	20	18,375	11,944
G.723r53	5300	40	11,385	7407
G.723r53	5300	20	17,490	11,389

© 2006 Cisco Systems, Inc. All rights reserved.
CVOICE v5.0-1-5

On average, an aggregate of 24 calls or more may contain 35 percent silence. With traditional telephony voice networks, all voice calls use 64-kbps fixed-bandwidth links regardless of how much of the conversation is speech and how much is silence. In Cisco VoIP networks, all conversations and silences are packetized. VAD suppresses packets of silence. Instead of sending VoIP packets of silence, VoIP gateways interleave data traffic with VoIP conversations to more effectively use network bandwidth.

VAD provides a maximum of 35 percent bandwidth savings based on an average volume of more than 24 calls.

Note Bandwidth savings of 35 percent is an average figure and does not take into account loud background sounds, differences in languages, and other factors.

The savings are not realized on every individual voice call, or on any specific point measurement.

Note For the purposes of network design and bandwidth engineering, VAD should *not* be taken into account, especially on links that will carry fewer than 24 voice calls simultaneously.

Various features, such as music on hold (MOH) and fax, render VAD ineffective. When the network is engineered for the full voice call bandwidth, all savings provided by VAD are available to data applications.

VAD is enabled by default for all VoIP calls. VAD reduces the silence in VoIP conversations but it also provides comfort noise generation (CNG). In some cases, silence may be mistaken for a disconnected call. CNG provides locally generated white noise to make the call appear normally connected to both parties.

Example: Span Engineering VAD Bandwidth Savings

Span Engineering is assessing the effect of VAD in a Frame Relay VoIP environment. The company plans to use G.729 for all voice calls crossing the WAN. Previously, it was determined that each voice call compressed with G.729 uses 26,400 bps. VAD can reduce the bandwidth utilization to 17,160 bps, which constitutes a bandwidth savings of 35 percent.

Practice Item: Span Engineering Voice Bandwidth Requirement

Span Engineering is planning to carry intrasite VoIP calls across the LAN at each site. The company plans to use the G.711 codec with a 30-ms voice sample for voice coding. Your task is to calculate how much bandwidth per call will be required to implement the design specifications.

1. Calculate the voice sample size in bytes, given that the codec will be G.711 with a 30-ms sample size.

2. Calculate the bandwidth per call for the G.711 call, including Ethernet overhead.

3. Calculate the bandwidth per call, including 35 percent VAD savings.

Practice Item Answer Key

1. Calculate the voice sample size in bytes, given that the codec will be G.711 with a 30-ms sample size.

$$\text{Bytes_per_Sample} = (\text{Sample_Size} * \text{Codec_Bandwidth}) / 8$$

$$\text{Bytes per sample} = (0.030 * 64,000) / 8$$

$$\text{Bytes per sample} = 240$$

2. Calculate the bandwidth per call for the G.711 call, including Ethernet overhead.

$$\text{Total_Bandwidth} = ([\text{Layer_2_Overhead} + \text{IP_UDP_RTP Overhead} + \text{Sample_Size}] / \text{Sample_Size}) * \text{Codec_Speed}$$

$$\text{Total bandwidth} = ([18 + 40 + 240] / 240) * 64,000$$

$$\text{Total bandwidth} = 79,467 \text{ bps}$$

3. Calculate the bandwidth per call, including 35 percent VAD savings.

$$\text{Total bandwidth} = \text{Bandwidth} - (\text{Bandwidth} * 35\%)$$

$$\text{Total bandwidth} = 79,467 - (79,467 * 0.35)$$

$$\text{Total bandwidth} = 51,653 \text{ bps}$$

Summary

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

Summary

- Different codecs have different bandwidth requirements.
- Voice sample size affects the bandwidth that is required.
- Overhead in Layer 2 protocols affects the bandwidth used.
- Security and tunneling adds significant overhead.
- Codec, Layer 2 protocol, sample size, and VAD must all be used when calculating VoIP bandwidth.
- VAD may lower bandwidth use up to 35 percent.

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-9

References

For additional information, refer to these resources:

- *Voice over IP – Per Call Bandwidth Consumption.*
http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.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) Which type of codec has the lowest bandwidth requirement?
- A) G.711
 - B) G.723
 - C) G.726
 - D) G.728
 - E) G.729
- Q2) Match the codec with the coding scheme that it uses.
- A) G.711
 - B) G.726
 - C) G.728
 - D) G.729
 - E) G.723
- _____ 1. ADPCM
- _____ 2. CS-ACELP
- _____ 3. LDCELP
- _____ 4. MPMLQ
- _____ 5. PCM
- Q3) What is the disadvantage of encapsulating more samples per PDU?
- A) Total bandwidth is reduced.
 - B) The delay becomes more variable.
 - C) More bandwidth is required.
 - D) The speed of the interface is reduced.
- Q4) What is the size of a voice sample from Cisco voice equipment using a G.728 codec?
- A) 10 ms
 - B) 20 ms
 - C) 24 ms
 - D) 40 ms
- Q5) What is the overhead for Frame Relay?
- A) 3 bytes
 - B) 5 bytes
 - C) 6 bytes
 - D) 18 bytes
- Q6) How many bytes in the Ethernet II overhead are used for CRC?
- A) 1 byte
 - B) 2 bytes
 - C) 4 bytes
 - D) 6 bytes

- Q7) What is the overhead associated with IPsec?
- A) 50 to 57 bytes
 - B) 24 bytes
 - C) 4 to 6 bytes
 - D) 6 bytes
- Q8) What is the overhead associated with MPLS?
- A) 50 to 57 bytes
 - B) 24 bytes
 - C) 4 bytes
 - D) 6 bytes
- Q9) Which three factors must be considered when calculating the total bandwidth of a VoIP call? (Choose three.)
- A) codec size
 - B) CRC usage
 - C) network-link overhead
 - D) sample size
 - E) capacity of network links
- Q10) What is the total bandwidth required for a 40-byte voice sample size using a G.729 codec and Frame Relay without CRTP?
- A) 9600 bps
 - B) 11,600 bps
 - C) 17,200 bps
 - D) 19,200 bps
- Q11) Which formula is used to calculate total bandwidth?
- A) $Total_Bandwidth = [Layer_2_Overhead + IP_UDP_RTP\ Overhead + Sample_Size] * Codec_Speed$
 - B) $Total_Bandwidth = ([Layer_2_Overhead + IP_UDP_RTP\ Overhead + Sample_Size] / Sample_Size) * Codec_Speed$
 - C) $Total_Bandwidth = ([Layer_3_Overhead + IP_UDP_RTP\ Overhead] / Sample_Size) * Codec_Speed$
 - D) $Total_Bandwidth = ([Layer_2_Overhead + IP_UDP_RTP\ Overhead + Sample_Size] / Sample_Size)$
 - E) $Total_Bandwidth = ([Layer_3_Overhead + IP_UDP_RTP\ Overhead + Sample_Size] / Sample_Size) * Codec\ Speed$
- Q12) What is the function of CNG?
- A) provides features such as MOH
 - B) provides white noise to make the call sound connected
 - C) provides full voice call bandwidth
 - D) reduces the delay in VoIP connections
- Q13) What is the bandwidth requirement if VAD is used when a voice call over Frame Relay is 11,395 bps?
- A) 3989 bps
 - B) 7407 bps
 - C) 9116 bps
 - D) 11,180 bps

Lesson Self-Check Answer Key

- Q1) B
Relates to: Codec Bandwidths
- Q2) 1-B
2-D
3-C
4-E
5-A
Relates to: Codec Bandwidths
- Q3) B
Relates to: Impact of Voice Samples and Packet Size on Bandwidth
- Q4) B
Relates to: Impact of Voice Samples and Packet Size on Bandwidth
- Q5) C
Relates to: Data-Link Overhead
- Q6) C
Relates to: Data-Link Overhead
- Q7) A
Relates to: Security and Tunneling Overhead
- Q8) C
Relates to: Security and Tunneling Overhead
- Q9) A, C, D
Relates to: Calculating the Total Bandwidth for a VoIP Call
- Q10) C
Relates to: Calculating the Total Bandwidth for a VoIP Call
- Q11) B
Relates to: Calculating the Total Bandwidth for a VoIP Call
- Q12) B
Relates to: Effects of VAD on Bandwidth
- Q13) B
Relates to: Effects of VAD on Bandwidth

Lesson 5

Allocating Bandwidth for Voice and Data Traffic

Overview

This lesson describes the importance of proper bandwidth engineering. Simply adding voice to an existing IP network is not acceptable. You must take proper precautions to ensure enough bandwidth for existing data applications and the additional voice traffic.

Relevance

Network administrators must be able to calculate existing bandwidth and forecast additional voice bandwidth that is required to implement Voice over IP (VoIP).

Objectives

Upon completing this lesson, you will be able to allocate bandwidth for voice and data traffic. This ability includes being able to meet these objectives:

- Describe the tools that are used to examine and collect traffic statistics
- Explain the network objectives for voice and data to ensure proper performance of the network
- Illustrate how to meet the network objectives within the current network
- Calculate the required number of trunks that are necessary to support voice traffic, considering the busy hour and dropped calls
- Calculate the busy hour traffic
- Describe erlangs as they relate to trunks
- Show three traffic probability assumptions when determining the number of trunks required to meet a grade of service
- Explain the purpose of traffic calculations
- Illustrate the creation of a call density matrix for calculating the trunk requirements between two points in a network
- Describe how to calculate the required bandwidth allocation for voice and data traffic

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Basic knowledge of VoIP
- Knowledge of TCP/IP networks

Outline

The outline lists the topics included in this lesson.

Outline

- Overview
- Sources of Traffic Statistics
- Network Objectives for Voice and Data
- Meeting the Current Network Objective
- Traffic Theory
- Busy Hour
- Erlangs
- Traffic Probability Assumptions
- Traffic Calculations
- Call Density Matrix
- Bandwidth Calculations
- Summary
- Lesson Self-Check

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1.2

Sources of Traffic Statistics

This topic describes the sources of traffic statistics for voice and data networks.

Sources of Traffic Statistics

- **Voice traffic statistics**
 - PSTN carrier
 - PBX CDR
 - Telephone bills
- **Data network statistics**
 - Network management systems
 - Sniffers
 - show interface commands
 - Router-based accounting

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v9.0-1-3

Traffic engineering, as it applies to traditional voice networks, involves determining the number of trunks that are necessary to carry a required number of voice calls during a specific time period. For designers of a voice network, the goal is to properly size the number of trunks and provision the appropriate amount of bandwidth that is necessary to carry the data equivalent of the number of trunks determined.

To determine the number of trunks, you must have statistics showing the current voice traffic.

Example: Gathering Statistics

You can gather voice traffic statistics from these sources:

- Public switched telephone network (PSTN) carriers
- Call Detail Records (CDRs) in PBXs
- Telephone bills

From the PSTN carrier, you can often gather the following information:

- **Peg counts:** Peg counts are for calls offered, calls abandoned, and all trunks busy. A peg count is a telephony term that dates back to the days of mechanical switches. A mechanical counter was attached to a peg to measure the number of events on that peg. The peg might be energized (sent a signal) for any one of several reasons, including call overflow and trunk seized. Today, electronic switches record peg counts by way of the software programs in their common control components.
- **Total traffic:** Total traffic is carried per trunk group.

In the absence of this detailed information, you could use a telephone bill to approximate the total traffic, but telephone bills do not show you the lost calls or the grade of service.

The internal telecommunications department provides CDRs for PBXs. This information typically records calls that are offered, but may not provide information on calls that were blocked because all trunks were busy.

Ideally, all call statistics are provided on a time-of-day basis. The number of trunks required to carry voice traffic is based on the *peak* daily traffic, not the *average* daily traffic.

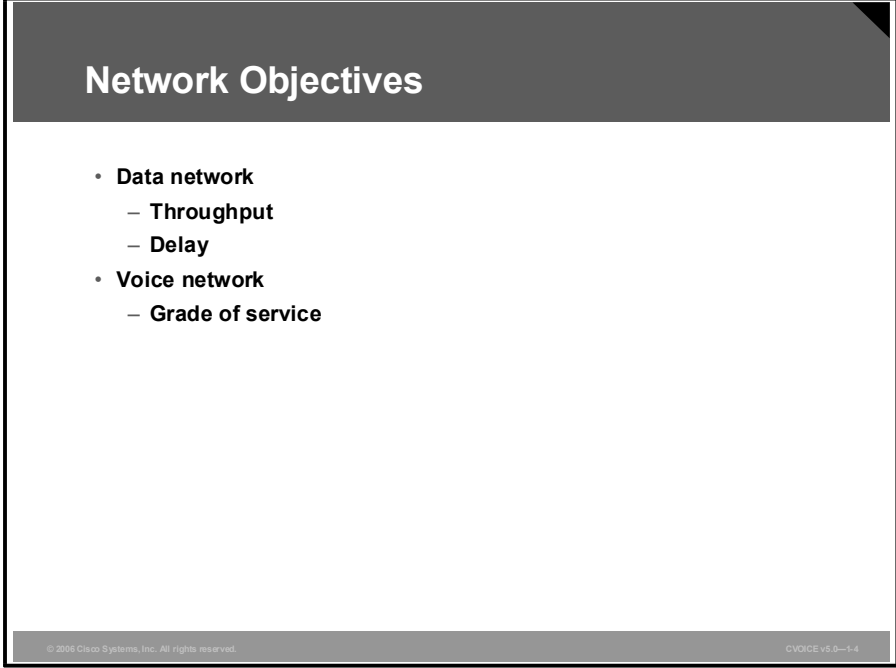
The total data traffic after migrating voice to the data network is the sum of the data traffic and the new voice traffic. The only exception is when the data network is accommodating voice and data on separate facilities. Therefore, you must know how much bandwidth is required for data application.

You can gather data traffic statistics from these sources:

- Network management systems (NMSs)
- Sniffers
- **show interface** commands
- Router-based accounting

Network Objectives for Voice and Data

This topic discusses the network objectives for voice and data to ensure proper performance of the network.



Network Objectives

- **Data network**
 - **Throughput**
 - **Delay**
- **Voice network**
 - **Grade of service**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v9.0-1-4

To provide an acceptable level of access to telephone and data services in a combined voice and data network, you must establish guidelines for the acceptable performance of each.

In a data network, users can reasonably expect to achieve a level of throughput in bits per second (bps) or a network transit delay in milliseconds (ms). Unfortunately, few networks have stated objectives for throughput and delay. In planning a combined voice and data network, voice is sharing the same paths as data. Voice is given first access to the network resources because of its real-time requirements. Service to the data users will be affected. You will be unable to judge the suitability of the combined voice and data network without a target for throughput and delay.

Traffic engineering for voice is based on a target grade of service. Grade of service is a unit that measures the chance that a call will be blocked. The grade of service is usually defined for the peak or busiest period in the business day when demand for service is at its highest. This approach means that the grade of service is naturally better during off-peak hours.

The grade of service is an important parameter when calculating the number of trunks required to carry a particular quantity of voice traffic.

Example: Grade of Service Value

For instance, a grade of service of P .01 means that one call is blocked in 100 call attempts, and a grade of service of P .001 results in one blocked call per 1000 attempts.

Meeting the Current Network Objective

This topic describes meeting the network objectives within the current network.

Meeting Objectives

- **Are the delay and throughput acceptable on the data network?**
- **Are you achieving grade of service on the voice network?**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-1-5

The first step is to measure the level of voice and data traffic in the networks and set the objectives for throughput, delay (data traffic), and grade of service (voice traffic). The next step is to determine whether you are meeting these objectives in the current network.

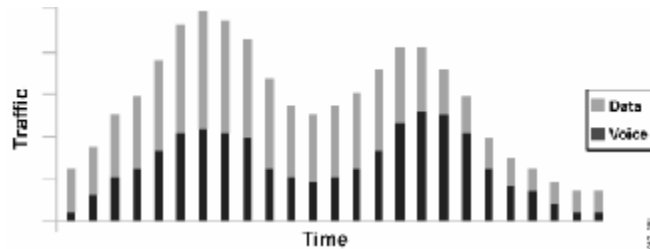
You may discover through your analysis of the voice and data networks that you are providing a poor grade of service to your voice users, or that the throughput and delay are below the standards for your data users. Without recognizing these shortcomings, you might be inclined to plan a combined network on the assumption of business as usual. This assumption is a mistake. It creates the very real possibility that you will have an integrated voice and data network that will be substandard to the original network.

You must ask two questions to determine if you are meeting current network objectives:

1. Are the delay and throughput acceptable on the data network?
2. Are you achieving grade of service on the voice network?

If you conclude that your network performance is below these objectives, add a factor to your current traffic analysis for excessive demand.

Network Demand



You must understand how voice and data network demands relate to each other. First you should look at the relationship between the peak demands on each of the networks if this information is available. It will give you some idea of what to expect later in this process, when you convert the number of voice trunks to bandwidth and add the voice bandwidth requirement to the data bandwidth for the same period. Clearly, the peak bandwidth demand is less if the two network demands are out of phase with each other than if both peaks coincide.

Example: Network Demand

Usually, networks will exhibit peak demands early in the morning and just after the noon hour. To best calculate the required bandwidth necessary to support demands, peak usage times must be understood.

Traffic Theory

This topic describes how to calculate the number of trunks necessary to support voice traffic.

Traffic Offered

A = C * T

- **Where:**
 - **A is the offered load.**
 - **C is the number of calls.**
 - **T is the average holding time of a call.**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-1-7

If you know the amount of traffic generated and the grade of service required, you can calculate the number of trunks required to meet your needs. Use the simple equation that follows to calculate traffic flow:

$$A = C * T$$

In the equation, A is the offered traffic, C is the number of calls originating during a period of one hour, and T is the average holding time of a call.

It is important to note that C is the number of calls *originated*, not carried. Typically, the information received from the carrier or from the internal CDRs of the company is in terms of *carried* traffic. Information provided by PBXs is usually in terms of *offered* traffic.

The holding time of a call (T) must account for the average time that a trunk is occupied and must factor in variables other than the length of a conversation. This includes the time required for dialing and ringing (call establishment), time to terminate the call, and a method of amortizing busy signals and noncompleted calls. Adding 10 percent to 16 percent to the length of an average call helps account for these miscellaneous time segments.

Hold times based on call billing records might have to be adjusted, based on the increment of billing. Billing records based on one-minute increments are usually rounded up to the *next* minute, not rounded to the *nearest* minute. Consequently, billing records overstate calls by 30 seconds on average; for example, a bill showing 404 calls (C) totaling 1834 minutes of traffic (A) should be adjusted as follows:

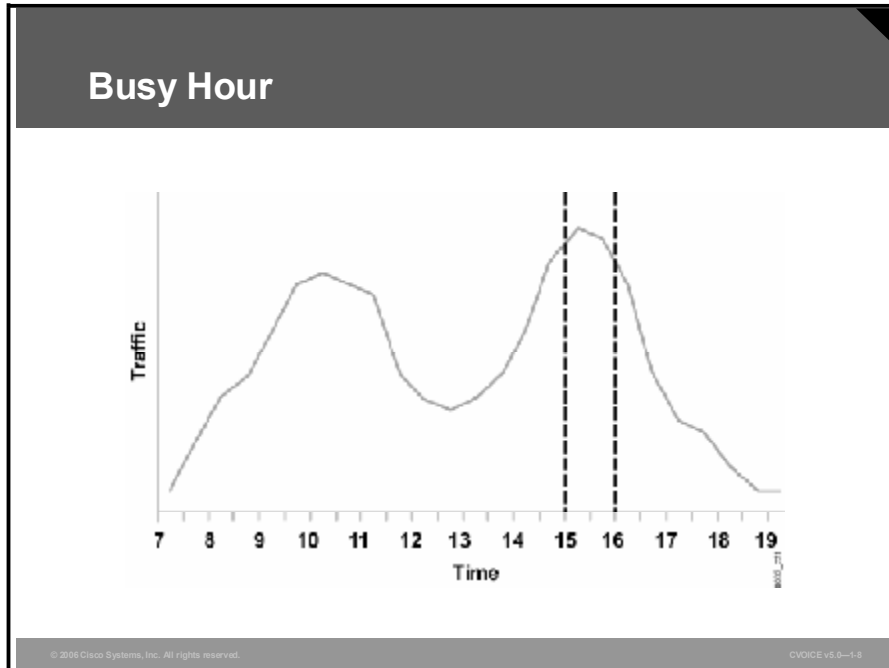
- $404 \text{ calls} * 0.5 \text{ minutes (overstated call length)} = 202 \text{ excess call minutes}$
- Adjusted traffic (A): $1834 - 202 = 1632 \text{ actual call minutes}$

Another way to calculate this would be to use the formula $A = C * T$ to derive the average holding time (T), reduce T by 0.5 minutes (the overstated amount), and recalculate the traffic offered (A).

- **Average holding time (T):**
 - $T = 1834 \text{ minutes (A)} / 404 \text{ calls (C)}$
 - $T = 4.54 \text{ minutes}$
- **Corrected holding time (T):**
 - $T = 4.54 - 0.50$
 - $T = 4.04 \text{ minutes}$
- **Adjusted traffic offered (A):**
 - $A = 404 \text{ calls (C)} * 4.04 \text{ minutes (T)}$
 - $A = 1632 \text{ call minutes}$

Busy Hour

This topic explains how to calculate the busy hour during any given day.



It is important to look at call attempts during the busiest hour of the day. The most accurate method of finding the busiest hour is to take the 10 busiest days in a year, sum up the traffic on an hourly basis, find the busiest hour, and then derive the average amount of time.

Determine the amount of traffic that occurs in a day based on 22 business days in a month and then multiply that number by 15 percent to 17 percent. As a rule, the busy hour traffic represents 15 percent to 17 percent of the total traffic that occurs in one day. Assume that you have a trunk group that carries 66,000 minutes in one month or 3000 minutes per day on average ($66,000/22$). You may then estimate the busy hour traffic by calculating 15 percent of the average daily traffic, or $3000 * 15\% = 450$ minutes.

Erlangs

This topic describes erlangs.

Erlangs

The amount of traffic a trunk can handle in one hour.

Equals:

- 60 call minutes
- 3600 call seconds
- 36 centum call seconds (CCS)

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0-1-9

The traffic volume in telephone engineering is measured in units called erlangs. An erlang is the amount of traffic that one trunk can handle in one hour. It is a nondimensional unit that has many functions.

Here are some of the other equivalent measurements that you might encounter:

1 erlang = 60 call minutes = 3600 call seconds = 36 centum call seconds (CCS)

Example: Erlang Calculation

On average, each user in a branch makes 10 calls with an average duration of 5 minutes during the busy hour. If the branch has 25 employees, the total minutes of call time during the busy hour is 10 calls per busy hour multiplied by 5 minutes per call multiplied by 25 employees per branch. The result is 1250 total call minutes. To find the erlangs, which is based on hours, divide 1250 by 60. This calculation gives you 20.83 erlangs.

Traffic Probability Assumptions

This topic explains three traffic probability assumptions to consider when determining the number of trunks that are required to meet a grade of service.

Assumptions

- **Potential sources**
- **Traffic arrival characteristics**
- **Lost calls**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-118

When you have determined the amount of traffic that occurs during the busy hour in erlangs, you can determine the number of trunks required to meet a particular grade of service. The number of trunks required differs, depending on these three traffic probability assumptions:

- **Number of potential sources:** There can be a major difference between planning for an infinite versus a small number of sources. As the number of sources increases, the probability of a wider distribution in the arrival times and holding times of calls increases. As the number of sources decreases, the ability to carry traffic increases.
- **Traffic arrival characteristics:** Usually, this assumption is based on a Poisson traffic distribution. This distribution was named after the mathematician who studied this concept extensively. Call arrivals follow a classic bell-shaped curve. You commonly use Poisson distribution for infinite traffic sources. The arrival characteristics of traffic (calls) may be classified as random, smooth, or bursty.
- **Treatment of lost calls:** What do you do when the station you are calling does not answer or all trunks are busy? Traffic theory considers these three possibilities:
 - **Lost Calls Cleared (LCC):** LCC assumes that once a call is placed and the server (network) is busy or not available, the call disappears from the system. In essence, you give up and do something different.
 - **Lost Calls Held (LCH):** LCH assumes that a call is in the system for the duration of the hold time, regardless of whether the call is placed. In essence, you continue to redial for as long as the hold time before giving up. Redialing is an important traffic consideration. Suppose that 200 calls are attempted. Forty calls receive busy signals and attempt to redial. That results in 240 call attempts, a 20 percent increase. The trunk group is now providing an even poorer grade of service than initially thought.

- **Lost Calls Delayed (LCD):** LCD means that when a call is placed, it remains in a queue until a server is ready to handle the call. Then LCD uses the server for the full holding time. This assumption is most commonly used for automatic call distribution (ACD) systems.

Note LCC tends to understate the number of trunks that are required; on the other hand, LCH overstates the number of trunks that are required.

Example: Traffic Arrival Assumption

Random arrivals are common with a large or infinite source of users whose calls are independent of each other. Assuming random arrivals, the probability of calls arriving during any particular time interval, such as the busy hour, is modeled by a Poisson distribution. Given the average number of calls per busy hour and the distribution of call-holding times, the Poisson distribution predicts the probability of zero calls, one call, two calls, and so on, up to the probability of a large number of calls arriving during the hour.

The characteristic bell shape of the distribution suggests that the probability of a few calls is low, as is the probability of a high number of calls. The peak probability represents the average. For example, if you have calculated the average number of calls during the busy hour to be 250, the Poisson distribution estimates the probability that you will receive 0 calls (very low probability), 100 calls (modest probability), 250 calls (the average, which is peak probability), 900 calls (very low probability), or any other number of calls.

Smooth traffic arrivals are common in applications in which the traffic is dependent on other traffic, as in a telemarketing scenario. Smooth traffic arrivals are not modeled on the Poisson distribution because of their nonrandom nature.

Bursty traffic arrivals are common in trunk overflow scenarios in which excess overflow tends to occur for a short time and then disappears for an extended period of time. Bursty traffic is not modeled on the Poisson distribution because of its nonrandom nature.

Traffic Calculations

This topic explains the purpose of traffic calculations.

Trunks	Probability of Lost Call					
	0.003	0.005	0.01	0.02	0.03	0.05
1	0.003	0.005	0.011	0.021	0.031	0.053
2	0.081	0.106	0.153	0.224	0.282	0.382
3	0.289	0.349	0.458	0.603	0.716	0.9
4	0.602	0.702	0.87	1.093	1.269	1.626
5	0.995	1.132	1.361	1.658	1.876	2.219
6	1.447	1.622	1.908	2.278	2.543	2.981
7	1.947	2.150	2.501	2.936	3.25	3.730
8	2.484	2.73	3.128	3.527	3.887	4.543
9	3.053	3.333	3.783	4.345	4.748	5.371
10	3.648	3.961	4.462	5.084	5.53	6.216
11	4.267	4.611	5.16	5.842	6.328	7.077
12	4.904	5.279	5.876	6.615	7.141	7.95
13	5.569	5.964	6.608	7.402	7.967	8.834
14	6.229	6.664	7.352	8.201	8.804	9.73
15	6.913	7.376	8.108	9.01	9.65	10.63

The purpose of traffic calculations is to determine the number of physical trunks that are required. After you have determined the amount of offered traffic during the busy hour, established the target grade of service, and recognized the three basic assumptions, you can calculate the number of trunks that are required by using formulas or tables.

Traffic theory consists of many queuing methods and associated formulas. Anyone who has taken a queuing theory class can testify to the complexity of the many queuing models that are derived for various situations. This is the reason why tables dealing with the most commonly encountered model are used.

The most commonly used model and table is Erlang B. Erlang B is based on infinite sources, LCC, and a Poisson distribution that is appropriate for either exponential or constant holding times. In general, Erlang B understates the number of trunks because of the LCC assumption. Erlang B is the most commonly used algorithm.

Example: Traffic Calculations

A trunk group is a hunt group of parallel trunks. This example determines the number of trunks in a trunk group carrying the following traffic:

- 352 hours of offered call traffic in a month
- 22 business days per month
- 10 percent call-processing overhead
- 15 percent of traffic occurs in busy hour
- Grade of service = P .01
- Busy hour = $352 / 22 * 15\% * 1.10$ (call-processing overhead) = 2.64 erlangs

The traffic assumptions are as follows:

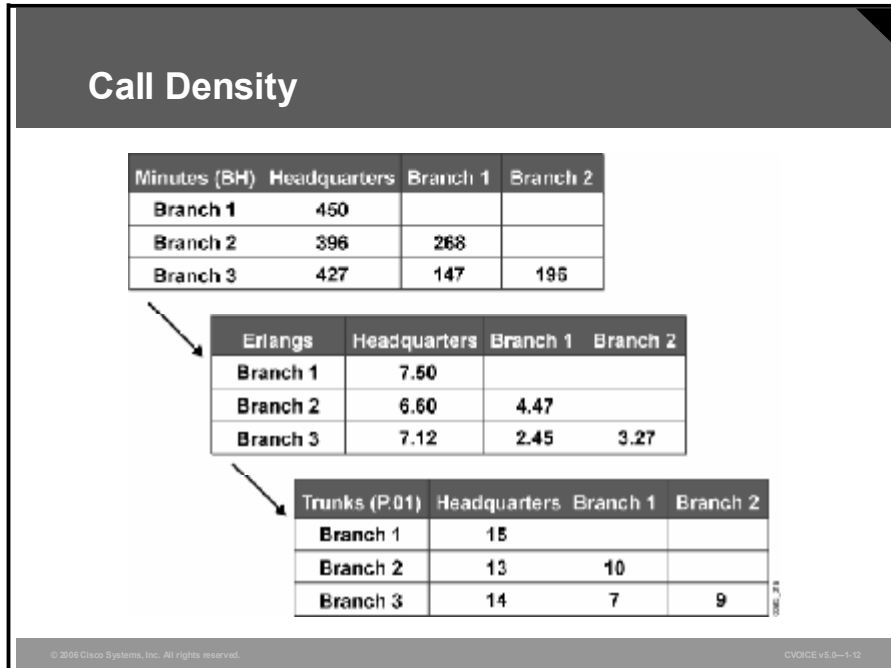
- Infinite sources
- Random or Poisson traffic distribution
- Lost calls are cleared

Based on these assumptions, the appropriate algorithm to use is Erlang B. You use the table in the Traffic Calculations figure to determine the appropriate number of trunks for a grade of service of P .01.

Because a grade of service of P .01 is required, you use the column that is designated as P .01 only. The calculations indicate a busy hour traffic amount of 2.64 erlangs, which is between 2.501 and 3.128 in the P .01 column. This corresponds to between seven and eight trunks. Because you cannot use a fractional trunk, use the next larger value of eight trunks to carry the traffic.

Call Density Matrix

This topic describes a call density matrix.



Unless your voice network is extremely small (two points, for example), calculating the trunk requirements between any two points in a network is a tedious task. One way to manage this more effectively is to design a “to and from” traffic matrix.

As you determine the call minutes between any two points, you enter the amount into the matrix. If you do this on a spreadsheet, you can convert the minutes to busy hour minutes, to erlangs, and then calculate the number of trunks from the erlangs. The number of trunks represents the number of concurrent calls that you should plan to support during the busy hour.

Example: Call Density Matrix

The figure shows this progression of spreadsheets for a network with one headquarters and three branches.

Bandwidth Calculations

This topic describes how to calculate the required bandwidth allocation for voice and data traffic.

VoIP Bandwidth					
Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with CRTP	Ethernet
	Bits per Second	Bytes	Bits per Second	Bits per Second	Bits per Second
G.711	64,000	240	76,267	66,133	79,467
G.711	64,000	160	82,400	67,200	87,200
G.726r32	32,000	120	44,267	34,133	47,467
G.726r32	32,000	80	50,400	35,200	55,200
G.726r24	24,000	80	37,800	26,400	41,400
G.726r24	24,000	60	42,400	27,200	47,200
G.726r16	16,000	80	25,200	17,600	27,600
G.726r16	16,000	40	34,400	19,200	39,200
G.728	16,000	80	25,200	17,600	27,600
G.728	16,000	40	34,400	19,200	39,200
G.729	8000	40	17,200	9600	19,600
G.729	8000	20	26,400	11,200	31,200
G.723r63	6300	48	12,338	7350	13,913
G.723r63	6300	24	18,375	8400	21,525
G.723r53	5300	40	11,395	6360	12,985
G.723r53	5300	20	17,490	7420	20,670

© 2006 Cisco Systems, Inc. All rights reserved. VOICE vs.0-1-10

If you are provisioning a circuit-switched voice network, you must estimate how much traffic each of your trunks is expected to carry. Then investigate the most cost-effective way to provision each of the trunks.

In this example, assume that all voice traffic is transported over the IP network. This approach will preclude the need to go through the rigors of choosing the most cost-effective solution for each individual trunk.

Determining IP Bandwidth

At this stage, the goal is to determine the IP bandwidth.

1. Estimate the VoIP bandwidth required for different coder-decoders (codecs) and over different data links. Also calculate the benefit of Compressed Real-Time Transport Protocol (CRTP). These estimates of bandwidth for VoIP are shown in the figure.
2. Identify the number of concurrent calls that you expect during the busy hour between points in the network. This should be a conservative approximation of the bandwidth required for voice. Simply multiply the number of concurrent calls by the bandwidth per call.

Bandwidth

Voice Bandwidth (kbps)	Headquarters	Branch 1	Branch 2
Branch 1	168		
Branch 2	145.6	112	
Branch 3	166.8	78.4	100.8

+

Data Bandwidth (kbps)	Headquarters	Branch 1	Branch 2
Branch 1	248		
Branch 2	216	63	
Branch 3	187	28	48

=

Total Bandwidth (kbps)	Headquarters	Branch 1	Branch 2
Branch 1	416		
Branch 2	361.6	175	
Branch 3	343.8	106.4	146.8

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-1-14

The spreadsheet shows the results for VoIP over a Frame Relay network using G.729 with CRTP. Each call requires 11.2 kbps.

You may want to consider some refinements to this simple multiplier. Consider the net benefits of bandwidth-reduction strategies, such as voice activity detection (VAD). VAD commonly reduces the bandwidth to between 60 percent and 70 percent of the original bandwidth. Just keep in mind that two animated talkers may not allow VAD to have any effect at all.

Finally, remember to combine the bandwidth budget for data applications with the bandwidth budget for voice.

Now you have the total bandwidth budget. You are ready to ensure that you do not overload the data links. You may be tempted at this point to believe that matching the access rate on an interface to the total bandwidth budget would be more cost-effective. Avoid this erroneous tactic.

On any network, as load approaches middle percentages, drops and delay exponentially increase. When designing networks to carry voice and data, peak bandwidth calculations should *not* equate to total bandwidth required for a given network link. For most business environments, you can use any of the following load levels as general rules for determining when a network is approaching excessive load:

- 20 percent of full capacity averaged over an 8-hour work day
- 30 percent averaged over the worst hour of the day
- 50 percent averaged over the worst 15 minutes of the day

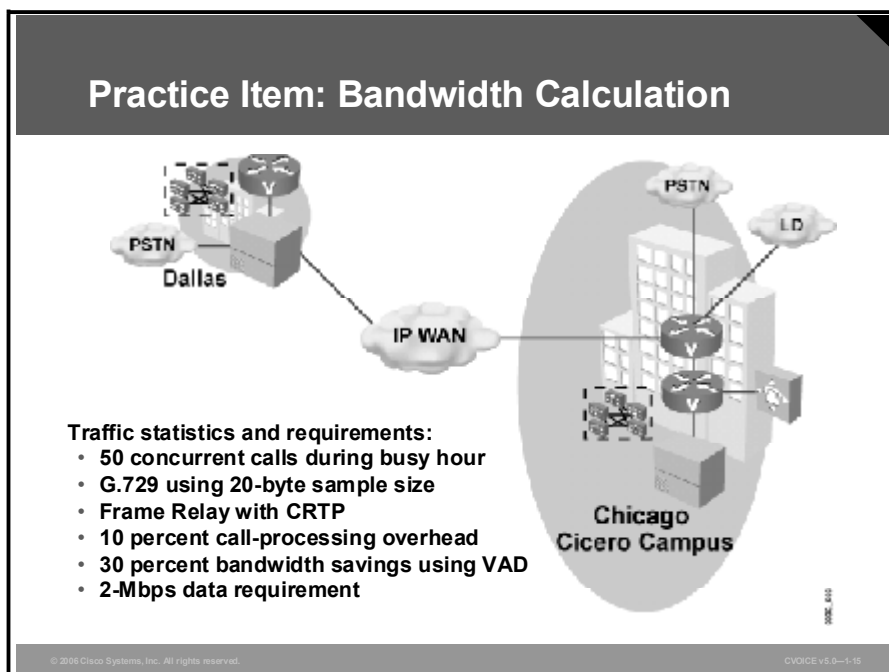
Capacity planning should take these factors into account, and link speed should be chosen to accommodate the proper load factors. An ideal goal is to have demand equal to about 35 percent of the total link speed.

To put these rules into the context of the example, the figure shows a demand for 416 kbps between the headquarters and Branch 1 during the busiest hour of the day. Using the rules, the average demand during the worst hour should represent only 30 percent of the link speed. If 30 percent of the link speed is 416 kbps, the link speed must be 1387 kbps or greater.

Based on the traffic in your network, you may justify aiming for a higher utilization of the links, but expecting full utilization is unrealistic. Setting too high a value will result in low throughput and high delay for data traffic. Voice is prioritized so that it is not delayed. You need to determine, through experience, a utilization factor that balances throughput and delay with cost.

Practice Item: Bandwidth Calculation

Span Engineering is assessing bandwidth requirements for the WAN connection between the Chicago Cicero campus and the Dallas campus. Use the traffic statistics and requirements in this diagram to determine the bandwidth requirements for the Cicero-Dallas connection.



Call statistics obtained from the PBXs and the PSTN carrier show that traffic patterns during the busy hour require support for 50 concurrent calls between Cicero and Dallas.

Design specifications for the Cicero-Dallas connection are as follows:

- All calls traversing the WAN must be compressed to conserve bandwidth and keep connection costs to a minimum.
- Calls traversing the WAN should be configured to use the G.729 codec with a 20-byte sample size.
- Calls traversing the WAN should be configured to use VAD. It is estimated that the use of VAD will save 30 percent of calculated voice bandwidth.
- The connection will be Frame Relay between Cicero and Dallas.
- The connection must have Real-Time Transport Protocol (RTP) header compression enabled.
- It is estimated that there will be a 10 percent overhead for call processing.
- The bandwidth requirement for data is 2 Mbps.

This table provides per-call bandwidth requirement calculations for a selection of codecs and connection types. Use this information for calculating total bandwidth requirements.

VoIP Bandwidth

Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with CRTP	Ethernet
	Bits per Second	Bytes	Bits per Second	Bits per Second	Bits per Second
G.711	64,000	240	76,267	66,133	79,467
G.711	64,000	160	82,400	67,200	87,200
G.726r32	32,000	120	44,267	34,133	47,467
G.726r32	32,000	80	50,400	35,200	55,200
G726r24	24,000	80	37,800	26,400	41,400
G.726r24	24,000	60	42,400	27,200	47,200
G.726r16	16,000	80	25,200	17,600	27,600
G.726r16	16,000	40	34,400	19,200	39,200
G.728	16,000	80	25,200	17,600	27,600
G.728	16,000	40	34,400	19,200	39,200
G.729	8000	40	17,200	9600	19,600
G.729	8000	20	26,400	11,200	31,200
G.723r63	6300	48	12,338	7350	13,913
G.723r63	6300	24	18,375	8400	21,525
G.723r53	5300	40	11,395	6360	12,985
G.723r53	5300	20	17,490	7420	20,670

1. Calculate the total bandwidth that is required for the expected concurrent call volume.

2. Calculate the total bandwidth that is required, including bandwidth needed for call-processing adjustment.

3. Calculate the total bandwidth that is required, including VAD savings.

4. Calculate the total bandwidth that is required for both voice and data for the Frame Relay connection.

Practice Item Answer Key

1. Calculate the total bandwidth that is required for the expected concurrent call volume.

For 50 concurrent calls, use G.729 for Frame Relay with CRTP:

$$50 * 11200 = 560000 \text{ (560 kbps)}$$

2. Calculate the total bandwidth that is required, including bandwidth needed for call processing adjustment.

Add call-processing overhead of 10 percent:

$$560000 * 110\% = 616000 \text{ (616 kbps)}$$

3. Calculate the total bandwidth that is required, including VAD savings.

Adjust for VAD bandwidth savings of 30 percent:

$$616000 - (30\% * 616000) = 616000 - 184800 = 431200 \text{ (431.2 kbps)}$$

4. Calculate the total bandwidth that is required for both voice and data for the Frame Relay connection.

Add data bandwidth requirements.

$$431200 + 2000000 = 2431200 \text{ (2.43 Mbps)}$$

Summary

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

Summary

- **Voice traffic statistics and data network statistics are among the sources of traffic statistics.**
- **The network objective for voice is measured in grade of service.**
- **To meet the current network objective, delay and throughput must be acceptable on the data network and grade of service must be achieved on the voice network.**
- **The equation $A = C * T$ is used to calculate traffic flow.**
- **Call volume should be measured during the busiest hour.**
- **Erlangs help determine trunk requirements.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-1-16

Summary (Cont.)

- **Three traffic probability assumptions to consider when determining the number of required trunks involve potential sources, traffic arrival characteristics, and lost calls.**
- **Traffic calculations can be used to determine the number of physical trunks required to meet grade of service.**
- **A call density matrix helps determine the number of trunks.**
- **Bandwidth required does not equal link speed.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-1-17

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 two goals of traffic engineering? (Choose two.)
- A) reduce the number of erlangs supported
 - B) properly size the number of trunks
 - C) provision the appropriate amount of bandwidth
 - D) double the peak demand
 - E) deny calls that exceed acceptable bandwidth
- Q2) Which source of traffic statistics can provide you with the most information?
- A) CDRs in PBXs
 - B) PSTN carriers
 - C) telephone bills
 - D) NMSs
- Q3) Which parameter is important for calculating the number of trunks required to carry voice traffic?
- A) throughput
 - B) delay
 - C) grade of service
 - D) packet loss
- Q4) Which type of statistic is measured by the grade of service?
- A) the delay variation of a call
 - B) the chance of a call being denied
 - C) the voice quality of a call
 - D) the chance of a call being blocked
- Q5) Which condition means that more bandwidth is required?
- A) The data network demand is less than the voice network demand.
 - B) The voice network demand is less than the data network demand.
 - C) The peak bandwidth demands of the voice and data networks coincide.
 - D) The peak bandwidth demands of the voice and data networks are out of phase.
- Q6) Which two factors determine whether data network requirements are being met? (Choose two.)
- A) acceptable grade of service
 - B) acceptable QoS
 - C) acceptable delay
 - D) acceptable packet loss
 - E) acceptable throughput
- Q7) In the equation $A = C * T$ used to calculate traffic flow, what does the C represent?
- A) number of calls originating during a one-hour period
 - B) number of calls carried during a one-hour period
 - C) average holding time for a call
 - D) length of an average call

- Q8) How much time must be added to the length of the actual call to get the holding time?
- A) half the length of the call
 - B) double the length of the call
 - C) 10 percent to 16 percent the length of the call
 - D) 10 percent to 16 times the length of the call
- Q9) What will be the busy hour traffic if the traffic for 1 month is 15,400 minutes?
- A) 77 minutes
 - B) 105 minutes
 - C) 116 minutes
 - D) 119 minutes
- Q10) What is the first measurement to take in a year, to which you will sum the traffic on an hourly basis, find the busiest hour, and derive the average amount of time to find the most accurate measurement of the busiest hour?
- A) the total number of days
 - B) the 10 busiest days
 - C) 22 business days
 - D) the 12 busiest days
- Q11) What is the equivalent of one erlang?
- A) 60 call seconds
 - B) 36 centum call seconds
 - C) 3600 centum call seconds
 - D) 1 minute
- Q12) What is the traffic volume in erlangs for a company with 30 employees who make an average of five 10-minute calls during the busy hour?
- A) 25 erlangs
 - B) 150 erlangs
 - C) 300 erlangs
 - D) 1500 erlangs
- Q13) Which three types of arrival traffic can be modeled on a Poisson distribution? (Choose three.)
- A) random arrivals
 - B) arrivals from a small number of sources
 - C) bursty arrivals
 - D) arrivals from an infinite number of sources
 - E) smooth arrivals
- Q14) Which traffic theory possibility overstates the number of trunks required with regard to the treatment of lost calls?
- A) LCC
 - B) LCD
 - C) LCH
 - D) LCL

- Q15) What is the most commonly used table for calculating the number of physical trunks required?
- A) Poisson distribution
 - B) Erlang B
 - C) grade of service algorithm
 - D) LCC table
- Q16) What are three traffic assumptions for the Erlang B algorithm? (Choose three.)
- A) fixed number of sources
 - B) random distribution
 - C) Lost Calls Delayed
 - D) Lost Calls Cleared
 - E) infinite sources
 - F) Lost Calls Held
- Q17) How many erlangs would be required with these assumptions?
- 733 hours of offered call traffic in a month
 - 22 business days per month
 - 5 percent call-processing overhead
 - 10 percent of the traffic occurs in the busy hour
 - grade of service = P .02
- A) 34.98
 - B) 3.498
 - C) 0.3498
 - D) 4.389
- Q18) How many trunks would be required with these assumptions?
- 450 hours of offered call traffic in a month
 - 22 business days per month
 - 10 percent call-processing overhead
 - 9 percent of the traffic occurs in the busy hour
 - grade of service = P .01
- A) 4
 - B) 5
 - C) 6
 - D) 7

- Q19) How many trunks would be required with these assumptions?
- 400 hours of offered call traffic in a month
 - 28 business days per month
 - 7 percent call-processing overhead
 - 2 percent of the traffic occurs in the busy hour
 - grade of service = P .01
- A) 3
B) 4
C) 5
D) 6
- Q20) What is an easy way to calculate the trunk requirements for a network?
- A) calculate the requirements between any two points and average them
B) calculate the requirements separately for each link
C) design a “to and from” traffic matrix
D) use the $A = C * T$ formula
- Q21) What do you calculate with the call density matrix?
- A) number of concurrent calls you should plan to support during the busy hour
B) number of calls you should plan to support during the day
C) total bandwidth of the calls that are on the network at any given time
D) number of calls that can be made without affecting voice quality of other calls
- Q22) What happens to drops and delays as traffic load approaches middle percentages?
- A) They increase for all traffic.
B) They decrease for all traffic.
C) They increase for data traffic only.
D) They decrease for voice traffic only.
- Q23) When doing capacity planning, what is the ideal goal for demand?
- A) average demand of 20 percent
B) average demand of 25 percent
C) average demand of 30 percent
D) average demand of 35 percent

Lesson Self-Check Answer Key

- Q1) B, C
Relates to: Sources of Traffic Statistics
- Q2) B
Relates to: Sources of Traffic Statistics
- Q3) C
Relates to: Network Objectives for Voice and Data
- Q4) D
Relates to: Network Objectives for Voice and Data
- Q5) C
Relates to: Meeting the Current Network Objective
- Q6) C, E
Relates to: Meeting the Current Network Objective
- Q7) A
Relates to: Traffic Theory
- Q8) C
Relates to: Traffic Theory
- Q9) B
Relates to: Busy Hour
- Q10) B
Relates to: Busy Hour
- Q11) B
Relates to: Erlangs
- Q12) A
Relates to: Erlangs
- Q13) A, C, E
Relates to: Traffic Probability Assumptions
- Q14) C
Relates to: Traffic Probability Assumptions
- Q15) B
Relates to: Traffic Calculations
- Q16) B, D, E
Relates to: Traffic Calculations
- Q17) B
Relates to: Traffic Calculations

- Q18) D
Relates to: Traffic Calculations
- Q19) A
Relates to: Traffic Calculations
- Q20) C
Relates to: Call Density Matrix
- Q21) A
Relates to: Call Density Matrix
- Q22) A
Relates to: Bandwidth Calculations
- Q23) D
Relates to: Bandwidth Calculations

Lesson 6

Considering Security Implications of VoIP Networks

Overview

This lesson describes the implications of implementing security measures in IP networks that transport voice.

Relevance

Security is a top priority in most networks. Security solutions include router access lists, stateful firewalls, and Virtual Private Networks (VPNs). These solutions may be standalone or layered. Implementing voice in a secure network environment requires an understanding of potential issues and threats. It also requires an in-depth knowledge of existing security measures and how those measures affect the transit of voice through the network.

Objectives

Upon completing this lesson, you will be able to describe the implications of implementing security measures in IP networks that will transport voice. This ability includes being able to meet these objectives:

- Explain the requirement for traffic security, network security, and intrusion detection to be included in VoIP network security policies
- Identify threats to VoIP environments
- Explain how assigning voice and data traffic to separate VLANs mitigates security risks
- Describe the dynamic access control process used by firewalls to allow voice packets to pass
- Outline the steps that are needed to reduce overhead and delay for VoIP in a VPN
- Calculate the bandwidth required for a VPN packet

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- General knowledge of VPNs
- General knowledge of VLANs
- General knowledge of firewalls
- Intermediate understanding of voice requirements, including delay and port numbering

Outline

The outline lists the topics included in this lesson.

Outline

- **Overview**
- **Security Policies for VoIP Networks**
- **Threats to VoIP Networks**
- **Secure LAN Design**
- **Communicating Through a Firewall**
- **Delivering VoIP over a VPN**
- **Bandwidth Overhead Associated with VPN**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-1-2

Security Policies for VoIP Networks

This topic describes the elements of a security policy for a VoIP network.

Elements of a Security Policy

- **Transport security:** Protect the data while it is in transit through the network
- **Network security:** Verify which data should be entering the network
- **Intrusion detection:** Provide notification in the event of unauthorized data detection

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v9.0-1-3

Numerous problems, from device failures to malicious attacks, affect the uptime of networks. With the reliance on the IP network for telephony, IP-based threats must be mitigated. Varying levels of security are available to suit individual corporate requirements. Here are some of the requirements for secured IP telephony:

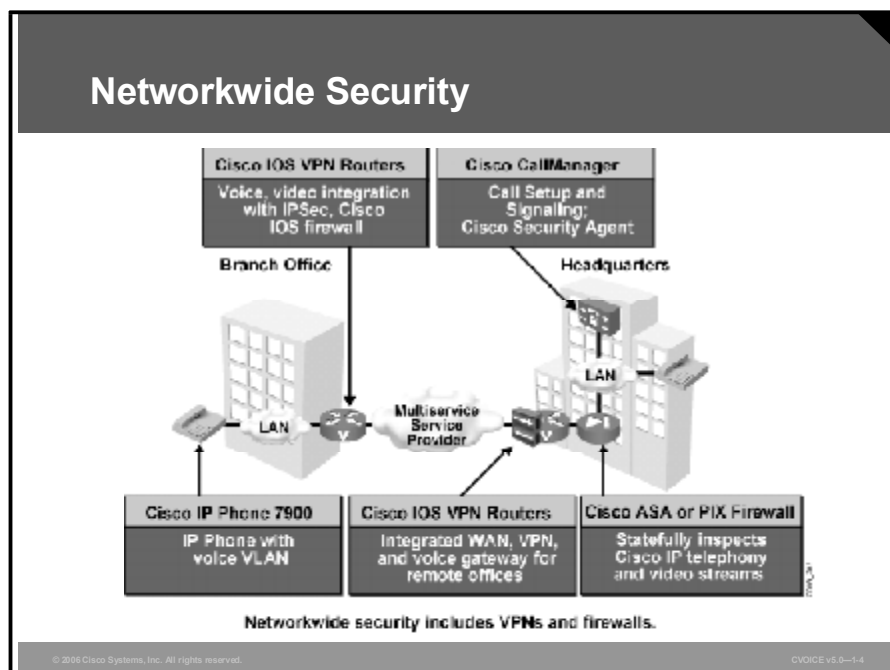
- Secured IP telephony must provide ubiquitous IP telephony services to the locations and to the users that require them.
- Secured IP telephony must maintain as many of the characteristics of traditional telephony as possible without compromising security
- Secured IP telephony must integrate with existing security architecture without interfering with existing functions.

The starting point for any security implementation is the development of a security policy. In a converged network, the security policy must account for the impact of security measures on voice traffic. The security policy should address the following points that affect voice:

- **Transport security:** Traffic traversing public access and backbone networks must be properly secured. IP Security (IPSec) and VPNs provide transport security by ensuring data confidentiality using encryption, data integrity, and data authentication between participating peers. Encryption adds to the overhead and delays the voice packet. You must factor in encryption when testing the delay budget and bandwidth calculations.

- Network security:** Cisco Systems firewalls provide stateful perimeter security that is critical to any public-facing network, such as a VPN. When deploying voice and video across VPNs, it is critical to statefully inspect all multiservice traffic traversing the firewall. Firewalls must be configured to allow known signal and payload ports to pass into the network. It is important to understand where the VPN terminates. If the VPN terminates inside the firewall, the traffic passing through the firewall is encrypted and is subject to stateful inspection. If the VPN terminates outside the firewall, the firewall has access to Real-Time Transport Protocol (RTP), User Datagram Protocol (UDP), TCP, or IP headers and is able to inspect the packet for call setup.
- Intrusion detection:** Cisco Security Agent provides threat protection for server and desktop computing systems, also known as endpoints. Cisco Security Agent identifies and prevents malicious behavior. This eliminates known and unknown security risks and helps to reduce operational costs. The Cisco Security Agent, by itself, aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall capabilities, malicious mobile code protection, operating system integrity assurance, and audit log consolidation. In addition, because Cisco Security Agent analyzes behavior rather than relying on signature matching, it reduces operational costs.

Example: Networkwide Security



In the figure, the network between the branch office and the headquarters has a firewall. The firewall allows the users from the branch office only to access the headquarters network. A user without proper network identification will not be allowed to pass through the firewall. Network identification protects voice networks from hackers.

The model chosen for IP voice networks today mirrors that chosen for legacy voice systems, which are generally wide open and require little or no authentication to gain access.

Threats to VoIP

This topic describes threats to Voice over IP (VoIP).

Threats to VoIP

- **Theft and toll fraud**
- **Unauthorized access to voice resources**
- **Compromise of network resources**
- **Downtime and DoS**
- **Invasion of call privacy**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-1-8

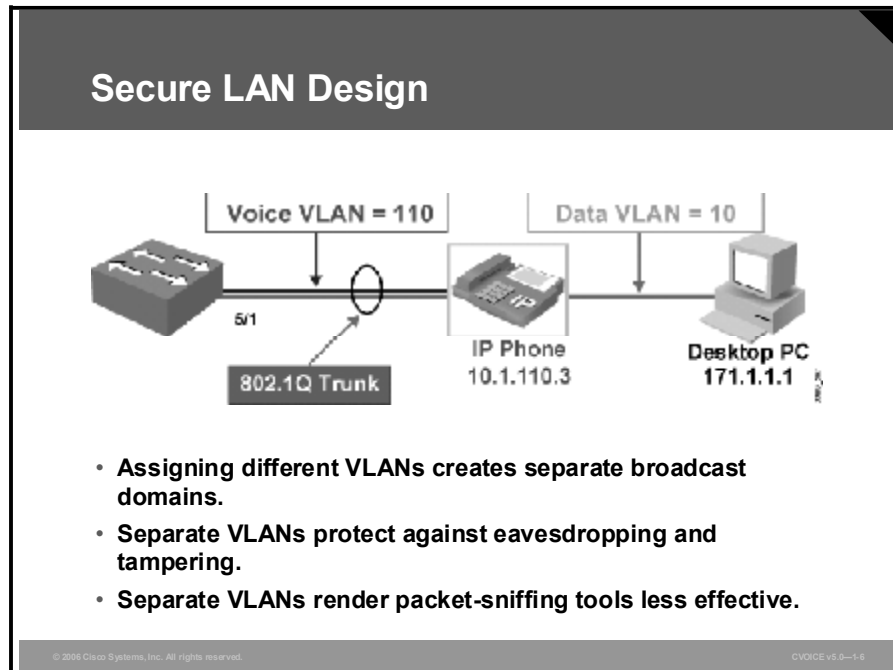
Here are some of the threats to VoIP networks:

- **Theft and toll fraud:** Toll fraud is the theft of long-distance telephone service by unauthorized access to a public switched telephone network (PSTN) trunk (an “outside line”) on a PBX or voice-mail system. Toll fraud is a multibillion-dollar illegal industry, and all organizations are vulnerable. Theft can also be defined as the use of the telephony system, by both authorized and unauthorized users, using voice network resources to access unauthorized numbers, such as 900 billable numbers.
- **Unauthorized access to voice resources:** Hackers can tamper with voice systems, user identities, and telephone configurations and also intercept voice-mail messages. If hackers gain access to the voice-mail system, they could change the voice-mail greeting, which will have a negative impact on the image and reputation of the company. A hacker who gains access to the PBX or voice gateway can shut down voice ports or change voice-routing parameters, affecting voice access into and through the network.
- **Compromise of network resources:** The goal of a secure network is to ensure that applications, processes, and users can reliably and securely interoperate using the shared network resources. Because the shared network infrastructure carries both voice and data, security and access to the network infrastructure is critical in securing voice functions. Because IP voice systems are installed on a data network, they are potential targets for hackers who previously targeted only PCs, servers, and data applications. Hackers are aided in their search for vulnerabilities in IP voice systems by the open and well-known standards and protocols used by IP networks.

- **Denial of service (DoS) attacks:** DoS attacks are defined as the malicious attacking or overloading of call-processing equipment to deny access to services by legitimate users. Most DoS attacks fall into one of these categories:
 - **Network resource overload:** This involves overloading a network resource that is required for proper functioning of a service. The network resource is most often bandwidth. The DoS attack uses up all available bandwidth, causing authorized users to be unable to access the required services.
 - **Host resource starvation:** This involves using up critical host resources. When use of these resources is maximized by the DoS attack, the server can no longer respond to legitimate service requests.
 - **Out-of-bounds attack:** This involves using illegal packet structure and unexpected data, which can cause the operating system of the remote system to crash. One example of this type of attack may be to use illegal combinations of TCP flags. Most TCP/IP stacks are developed to respond to appropriate use: they are not developed for anomalies. When the stack receives illegal data, it may not know how to handle the packet and may cause a system crash.
- **Eavesdropping:** Eavesdropping involves the unauthorized interception of voice packets or RTP media streams. Eavesdropping exposes confidential or proprietary information that is obtained by intercepting and reassembling packets in a voice stream. Numerous tools are used by hackers to eavesdrop.

Secure LAN Design

This topic describes key points of secure LAN design.



Many IP security solutions can be implemented only on Layer 3 (IP) devices. Because of protocol architecture, the MAC layer, Layer 2, offers very little or no inherent security. Understanding and establishing broadcast domains is one of the fundamental precepts in designing secure IP networks. Many simple yet dangerous attacks can be launched if the attacking device resides within the same broadcast domain as the target system.

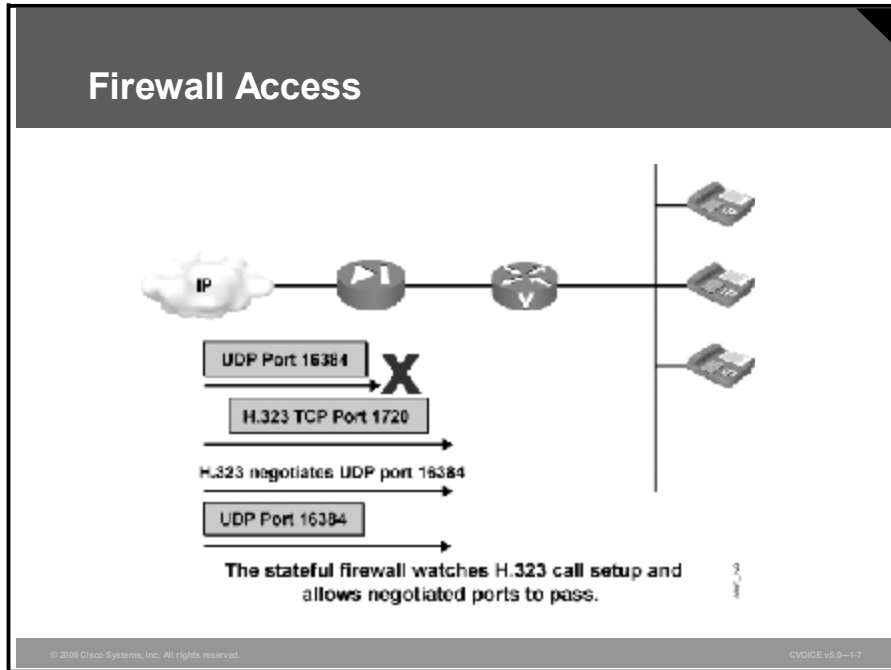
The IP phones, VoIP gateways, and network management workstations should always be on their own subnetwork, separate from the rest of the data network and from each other.

To ensure communications privacy and integrity, voice media streams must be protected from eavesdropping and tampering. Data-networking technologies such as VLANs can segment voice traffic from data traffic, preventing access to the voice VLAN from the data VLAN. Using separate VLANs for voice and data in a switched Ethernet infrastructure prevents any attacker or attacking application from snooping or capturing other VLAN Ethernet traffic as it traverses the physical wire. By making sure that each device connects to the network using a switched infrastructure, you can render packet-sniffing tools less effective for capturing user traffic.

Assigning voice traffic to specific VLANs to logically segment voice and data traffic is an industry-wide accepted best practice. As much as possible, devices identified as voice devices should be restricted to dedicated voice VLANs. This approach will ensure that they can communicate only with other voice resources. More importantly, voice traffic is kept away from the general data network where it might more easily be intercepted or tampered with.

Communicating Through a Firewall

This topic describes how voice is transmitted through a firewall.



Firewalls inspect packets and match them against configured rules. It is difficult to specify ahead of time which ports will be used in a voice call because they are dynamically negotiated during call setup.

H.323 is a complex, dynamic protocol that consists of several interrelated subprotocols. The ports and addresses used with H.323 require detailed inspection as call setup progresses. As the dynamic ports are negotiated, the firewall must maintain a table of current ports associated with the H.323 protocol. As calls are torn down, the firewall must remove those ports from the table. The process of removing ports from the table is called "stateful inspection of packets." In addition to checking static ports and recognizing protocols that negotiate dynamic ports as in H.323, the firewall looks into the packets of that protocol to track the flows.

Example: Stateful Firewall

Any application may use a port in the range of 1024 to 65536. In the figure, the firewall initially blocks all packets destined for UDP port 16384. The firewall becomes H.323-aware when it is configured to look for TCP port 1720 for call setup and UDP port assignments.

The table illustrates the dynamic access control process used by firewalls.

Dynamic Access Control

Stage	What Happens
The firewall detects a new call setup destined for UDP port 16384.	The firewall places the port, the associated source, and the destination IP address into the table.
The firewall opens port 16384.	The firewall allows all packets with UDP port 16384 and the proper source/destination IP address through the firewall.
The firewall detects call teardown.	The firewall removes the ports from the list, and the packets destined for the UDP port are blocked.

If the firewall does not support this dynamic access control based on the inspection, an H.323 proxy can be used. The H.323 proxy passes all H.323 flows to the firewall with the appearance of a single static source IP address plus TCP/UDP port number. The firewall can then be configured to allow that static address to pass through.

Firewalls can introduce variable delay into the path of the voice packet. It is extremely important that you ensure that the firewall has the proper resources to handle the load.

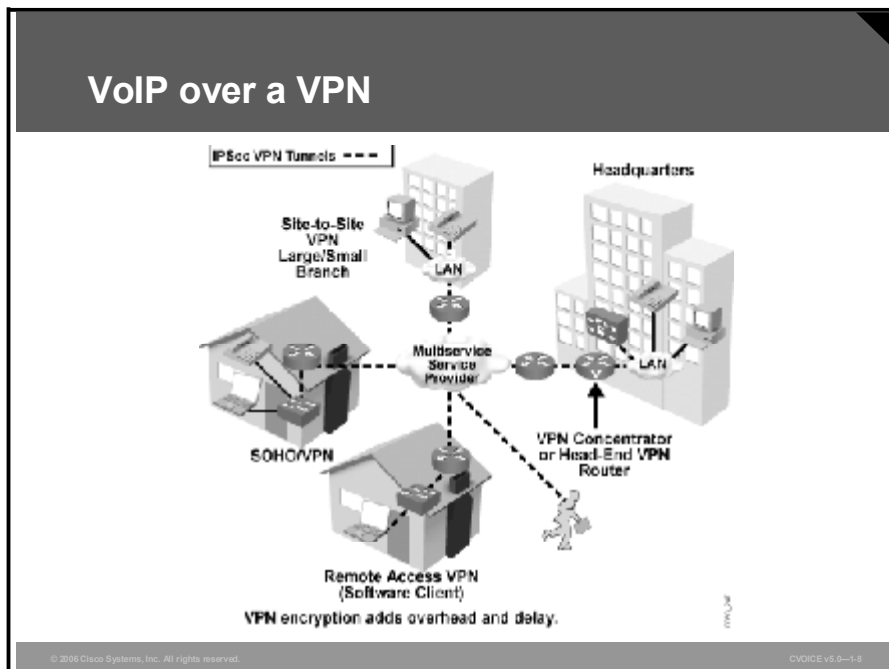
The table lists the ports used for various voice protocols.

Voice Protocol Ports

Protocol	Ports	TCP/UDP	Description
H.323	1718	UDP	Gatekeeper discovery
H.323	1719	UDP	Gatekeeper registration
H.323 (H.225)	1720	TCP	Call setup
Media Gateway Control Protocol MGCP (MGCP)	2427, 2727	UDP	MGCP gateway, MGCP call agent
Session initiation protocol(SIP)	5060	TCP or UDP	SIP call
Skinny Client Control Protocol (SCCP)	2000	TCP	Client
SCCP	2001	TCP	Digital gateway
SCCP	2002	TCP	Analog gateway
SCCP	2003	TCP	Conference bridge

Delivering VoIP over a VPN

This topic explains how to optimize the delivery of VoIP through a VPN.



VPNs are widely used to provide secure connections to the corporate network. The connections can originate from a branch office, a small office/home office (SOHO), a telecommuter, or a roaming user.

Frequently asked questions about voice over VPN generally deal with overhead and delay, which have an impact on the quality of service (QoS) for the call.

Note One important consideration to remember is the absence of QoS when deploying VPNs across the Internet or a public network. Where possible, QoS should be addressed with the provider through a service level agreement (SLA). An SLA is a document that details the expected QoS parameters for packets transiting the provider network.

Voice communications do not work with latency, not even a modest amount of it. Because secure VPNs encrypt data, they may create a throughput bottleneck when they process packets through their encryption algorithm. The problem usually gets worse as security increases. For example, Triple Data Encryption Standard (3DES) uses a long, 168-bit key. 3DES requires that each packet be encrypted three times, effectively tripling the encryption overhead.

The table describes how to reduce overhead and delay in VPNs.

Reducing Overhead and Delay

Step	Action
1.	Optimize the encryption algorithm and data path.
2.	Handle all processing in a dedicated encryption processor.
3.	Ensure that the device uses hardware encryption instead of software encryption.
4.	Use proper QoS techniques.
5.	Use proper VPN technologies.

VoIP can be secure and free of perceptible latency on a VPN. The solution is to optimize the encryption algorithm and the data path and to handle all processing in a dedicated encryption processor. You must ensure that the device is utilizing hardware encryption instead of software encryption. Software encryption relies on CPU resources and could severely impact voice quality.

Delay can be further minimized through use of proper QoS techniques. QoS and bandwidth management features allow a VPN to deliver high transmission quality for time-sensitive applications, such as voice and video. Each packet is tagged to identify the priority and time sensitivity of its payload, and traffic is sorted and routed based on its delivery priority. Cisco VPN solutions support a wide range of QoS features.

It is important to understand that QoS cannot be completely controlled, independent of the underlying network. QoS is only as good as the network through which the voice travels. Users must confirm with a potential service provider that the network can support priority services over a VPN. SLAs with carriers can guarantee expectations of network stability and QoS.

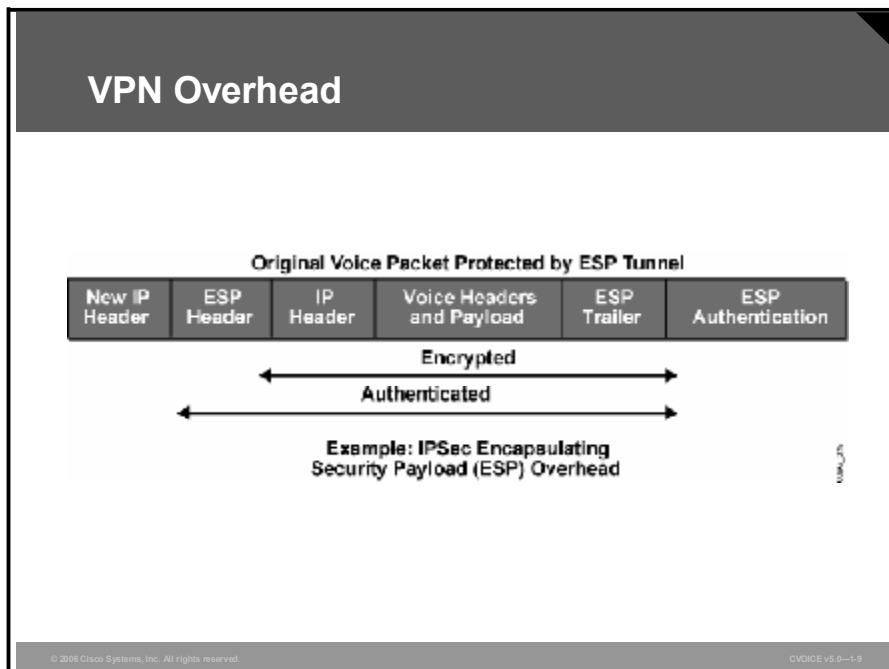
Overhead can be minimized if you understand the proper use of VPN technologies. VPNs can be implemented at Layer 2 through Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP), as well as at Layer 3 with IPSec. Often Layer 2 and Layer 3 technologies are combined to provide additional security. It is crucial that you understand the reasoning and requirements behind combining Layer 2 with Layer 3 security, because the combination adds overhead to the VoIP packet.

International Issues

VoIP and either Data Encryption Standard (DES) or 3DES encryptions are fully compatible with each other as long as the VPN delivers the necessary throughput. Internationally, corporations can run into other factors. The U.S. Department of Commerce places restrictions on the export of certain encryption technology. Usually, DES is exportable while 3DES is not, but regulations generality takes numerous forms, from total export exclusions applied to certain countries to allowing 3DES export to specific industries and users. Most corporations with VPNs that extend outside the United States should find out if their VPN provider has exportable products and how export regulations impact networks built with those products.

Bandwidth Overhead Associated with a VPN

This topic discusses the bandwidth overhead associated with a VPN.



VPN implementations vary, and there are many options to explore.

IPSec is the predominant VPN in use today. Generally, IPSec encrypts or authenticates, or both, the IP packet and adds additional headers to carry the VPN information. The VPN places the original IP packet into another IP packet so that the original information, including headers, is not easily seen or read.

To properly calculate bandwidth overhead, the user must have a thorough understanding of the VPN technology by asking these questions:

- Should the VPN be a Layer 2 tunnel running PPTP or L2TP?
- Should the VPN be a Layer 3 tunnel running IPSec?
- If the VPN is IPSec, is it using Authentication Header (AH) or Encapsulating Security Payload (ESP)?
- If the VPN is running AH or ESP, is it in transport mode or tunnel mode?

Example: VPN Bandwidth

The VPN adds a new IP header that is 20 bytes, plus the VPN header, which can add as much as 20 bytes to 60 bytes more, depending on which variation of VPN is installed. The table shows what a complete VPN packet can look like.

VPN Packet

Field	Subhead
Voice payload (G.729)	20 bytes
RTP header	12 bytes
UDP header	8 bytes
IP header	20 bytes
VPN header	20 bytes to 60 bytes
New IP header	20 bytes

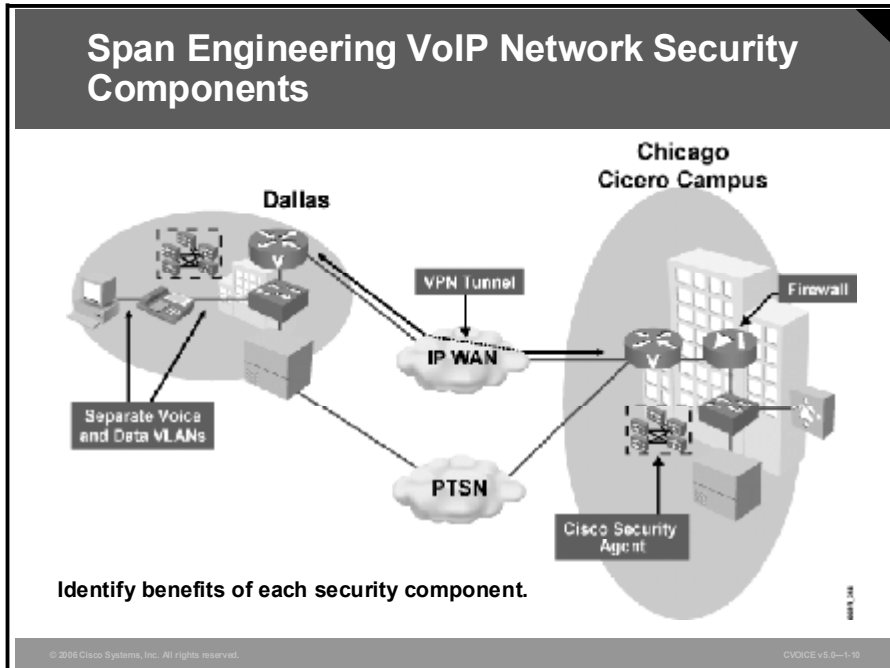
The total size of the packet will be 100 bytes to 160 bytes.

To calculate the total bandwidth for a 160-byte G.729 packet, use these calculations:

- Total bandwidth = 160 bytes * 8 = 1280 bits
- Total bandwidth = 1280 bits / 20 ms
- Total bandwidth = 64,000 bps

Practice Item: Span Engineering VoIP Network Security Components

Span Engineering is defining its security infrastructure for the VoIP network. This diagram identifies various components that will provide networkwide security for Span Engineering voice transmissions.



Your task is to identify the benefits associated with each security component.

1. Separate voice and data VLANs:

2. VPN connectivity between sites:

3. Stateful firewall:

4. Cisco Security Agent:

Practice Item Answer Key

1. Separate voice and data VLANs:
 - Separate VLANs create separate broadcast domains.
 - Separate VLANs protect against eavesdropping and tampering.
 - Separate VLANs render packet-sniffing tools less effective.

2. VPN connectivity between sites:
 - Voice packets are encrypted when they traverse the WAN.

3. Stateful firewall:
 - Firewalls inspect packets and match them against a set of rules.
 - Stateful firewalls watch call setup packets and let negotiated ports pass through.
 - Stateful firewalls tear down access to negotiated ports when the call is terminated.

4. Cisco Security Agent:
 - Cisco Security Agent provides intrusion detection for the network.
 - Cisco Security Agent identifies and prevents malicious behavior.

Summary

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

Summary

- **Security policies must encompass both transport and network security and should recommend monitoring for intrusion detection.**
- **Security threats against VoIP include toll fraud, invasion of privacy, unauthorized access to resources, and DoS attacks.**
- **Separate VLANs for voice and data prevent eavesdropping and tampering.**
- **Stateful firewalls inspect voice signaling packets to determine which UDP ports to allow through. Firewalls that are not capable of stateful inspection require the presence of an H.323 proxy server.**
- **VPN encryption headers introduce additional overhead that negatively impacts voice traffic.**
- **To calculate bandwidth overhead, you must understand the VPN technology and protocols.**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE vs.0-1-11

References

For additional information, refer to these resources:

- *SAFE VPN: IPsec Virtual Private Networks in Depth.*
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm
- 1. *Security Architecture for the Internet Protocol* (IETF Network Working Group Memo on RFC 2401). <http://www.ietf.org/rfc/rfc2401.txt?number=2401>.
- Cisco SAFE Blueprint.
http://www.cisco.com/en/US/partner/netsol/ns340/ns394/ns171/ns128/networking_solution_s_package.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) A converged network security policy should address which three points? (Choose three.)
- A) intrusion detection
 - B) application policy
 - C) transport security
 - D) network security
 - E) WAN access security
- Q2) Which feature provides transport security for a VoIP network?
- A) encryption and data authentication
 - B) inspection of traffic at the firewall
 - C) proactive notification of an attempted attack
 - D) intrusion detection
- Q3) Which situation allows the firewall to inspect the packet for call setup?
- A) The firewall is configured for call setup.
 - B) The VPN terminates outside the firewall.
 - C) The VPN terminates inside the firewall.
 - D) The firewall does not recognize the signal or payload ports.
- Q4) What are two ways that DoS attacks affect voice networks? (Choose two.)
- A) overload available bandwidth with unauthorized packets
 - B) provide access to change voice greeting in voice-mail systems
 - C) cause unauthorized use of resources in voice devices and servers
 - D) provide access to long distance trunks for unauthorized 900 billable calls
 - E) reconfigure VoIP telephone settings
- Q5) How is eavesdropping accomplished in a VoIP network?
- A) viewing of call detail record log files
 - B) connecting an analog telephone to a gateway and duplicating a telephone number
 - C) using tools that intercept and reassemble voice packet streams
 - D) gaining unauthorized access to a voice gateway
- Q6) Which method is used to place voice into a separate broadcast domain from data?
- A) connect all VoIP telephones through a wiring closet dedicated only to voice ports
 - B) configure all VoIP telephones in a different IP subnetwork
 - C) avoid use of trunks in a voice switch
 - D) configure all VoIP telephones to be in a separate VLAN

- Q7) What is one benefit of placing voice and data into separate VLANs?
- A) It isolates voice traffic from data traffic, which renders sniffing tools ineffective.
 - B) It ensures that voice traffic will not affect data traffic in the network.
 - C) Each VLAN port can be configured to run in full-duplex mode.
 - D) It allows data traffic to be prioritized.
- Q8) Which ports does the firewall include in the list of ports that are allowed access?
- A) all TCP and UDP ports
 - B) ports that are configured on the firewall
 - C) ports that were used during past call setups
 - D) ports that are currently being used for call setup
- Q9) What can you do if the firewall does NOT support dynamic access control?
- A) use a different protocol
 - B) use an H.323 proxy
 - C) configure the firewall for all possible ports
 - D) use static port numbers for call setup and teardown
- Q10) When compared to software encryption, how does hardware encryption reduce overhead and delay?
- A) It optimizes the encryption algorithm and data path.
 - B) It handles all processing in a dedicated compression engine.
 - C) It does not rely on CPU resources.
 - D) It uses proper QoS technologies.
- Q11) Which three encryption technologies can be used on international networks? (Choose three.)
- A) DES
 - B) 3DES
 - C) ESP
 - D) IPSec
 - E) IDEA
- Q12) How many bytes of overhead does VPN add to the voice packet?
- A) 20 bytes
 - B) 40 bytes
 - C) 20 bytes to 60 bytes
 - D) 40 bytes to 80 bytes
- Q13) Which type of VPN is most commonly used today?
- A) IPSec
 - B) ESP
 - C) PPTP
 - D) L2TP

Lesson Self-Check Answer Key

- Q1) A, C, D
Relates to: Security Policies for VoIP Networks
- Q2) A
Relates to: Security Policies for VoIP Networks
- Q3) B
Relates to: Security Policies for VoIP Networks
- Q4) A, C
Relates to: Threats to VoIP
- Q5) C
Relates to: Threats to VoIP
- Q6) D
Relates to: Secure LAN Design
- Q7) A
Relates to: Secure LAN Design
- Q8) D
Relates to: Communicating Through a Firewall
- Q9) B
Relates to: Communicating Through a Firewall
- Q10) C
Relates to: Delivering VoIP over a VPN
- Q11) A, C, D
Relates to: Delivering VoIP over a VPN
- Q12) C
Relates to: Bandwidth Overhead Associated with VPN
- Q13) A
Relates to: Bandwidth Overhead Associated with VPN

Module 2

Configuring Voice Networks

Overview

In this module, you will learn basic configuration of analog and digital voice ports. You will learn how to fine-tune voice ports with port-specific configurations. You will also learn how to configure voice port network connections and dial peers for plain old telephone service (POTS) and Voice over IP (VoIP) calls.

Module Objectives

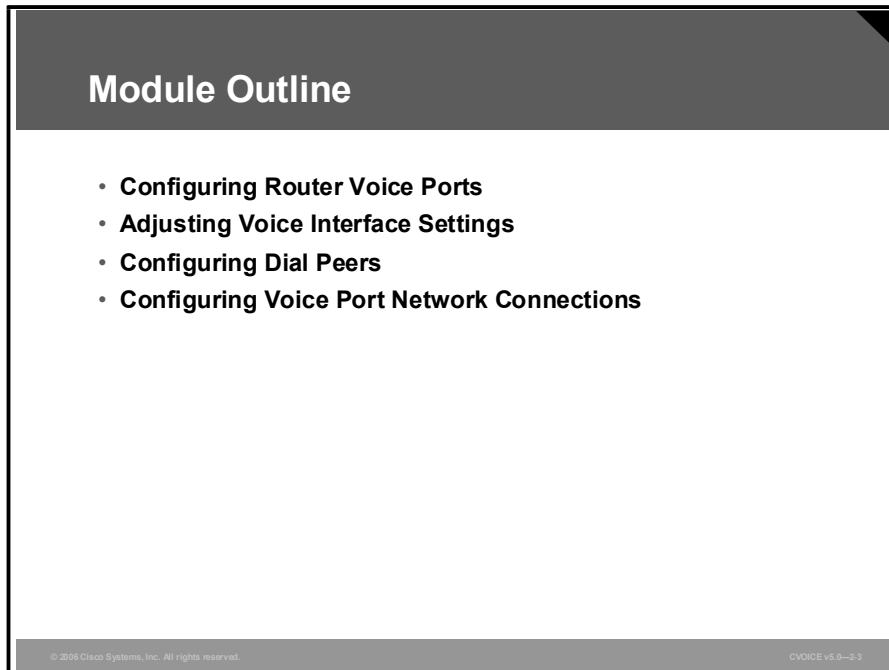
Upon completing this module, you will be able to configure voice interfaces on Cisco voice-enabled equipment for connection to traditional, nonpacketized telephony equipment. You will be able to define and configure POTS and VoIP dial peers. You will also be able to configure voice ports for various connection types.

Module Objectives

- **Configure analog and digital voice interfaces as new devices are introduced into the voice path**
- **Configure analog and digital voice ports for optimal voice quality**
- **Configure POTS and VoIP dial peers**
- **Configure voice port connections**

Module Outline

The outline lists the components of this module.

A slide titled "Module Outline" with a list of four topics: "Configuring Router Voice Ports", "Adjusting Voice Interface Settings", "Configuring Dial Peers", and "Configuring Voice Port Network Connections". The slide has a dark grey header and footer.

Module Outline

- **Configuring Router Voice Ports**
- **Adjusting Voice Interface Settings**
- **Configuring Dial Peers**
- **Configuring Voice Port Network Connections**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2.3

Lesson 1

Configuring Router Voice Ports

Overview

This lesson details the configuration parameters and troubleshooting commands for analog and digital voice ports.

Relevance

Connecting voice devices to a network infrastructure requires an in-depth understanding of the signaling and electrical characteristics that are specific to each type of interface. Improperly matched electrical components can cause echo and make a connection unusable. Configuring devices for international implementation requires knowledge of country-specific settings. This lesson provides voice port configuration parameters for signaling and country-specific settings.

Objectives

Upon completing this lesson, you will be able to configure analog and digital voice interfaces as new devices are introduced into the voice path. This ability includes being able to meet these objectives:

- Provide examples of seven types of voice port applications
- Set the configuration parameters for FXS voice ports
- Set the configuration parameters for FXO voice ports
- Set the configuration parameters for E&M voice ports
- Set timers and timing requirements on ports to adjust the time allowed for specific functions
- Set the configuration parameters for digital voice ports
- Set the configuration parameters for ISDN voice ports
- Configure T-CCS in a VoIP environment
- Use the **show**, **debug**, and **test** commands to monitor and troubleshoot voice ports

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Familiarity with Cisco IOS commands
- Familiarity with analog and digital voice port usage

Outline

The outline lists the topics included in this lesson.

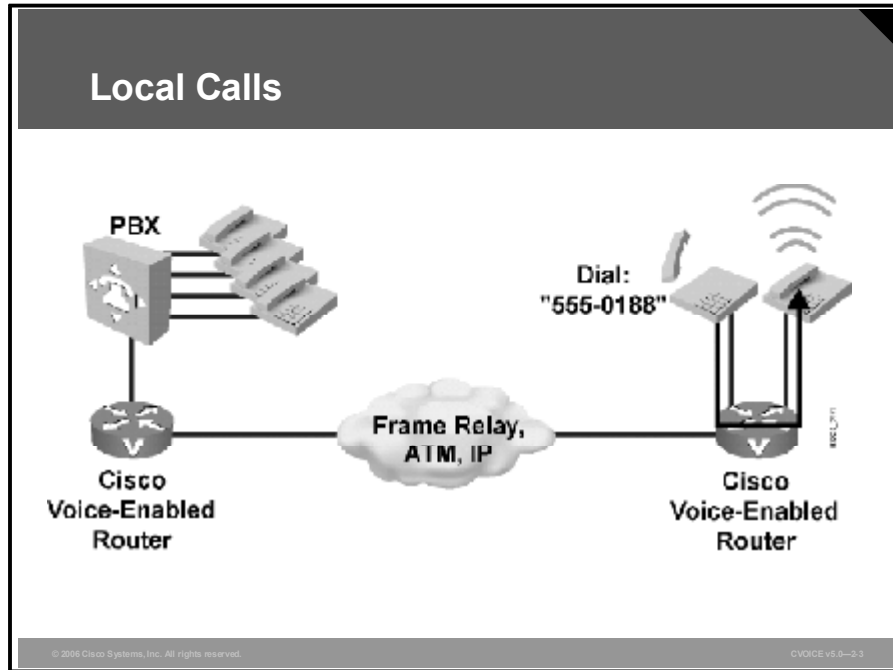
Outline

- Overview
- Voice Port Applications
- FXS Ports
- FXO Ports
- E&M Ports
- Timers and Timing
- Digital Voice Ports
- ISDN
- CCS Options
- Monitoring and Troubleshooting
- Summary
- Lesson Self-Check

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-2.2

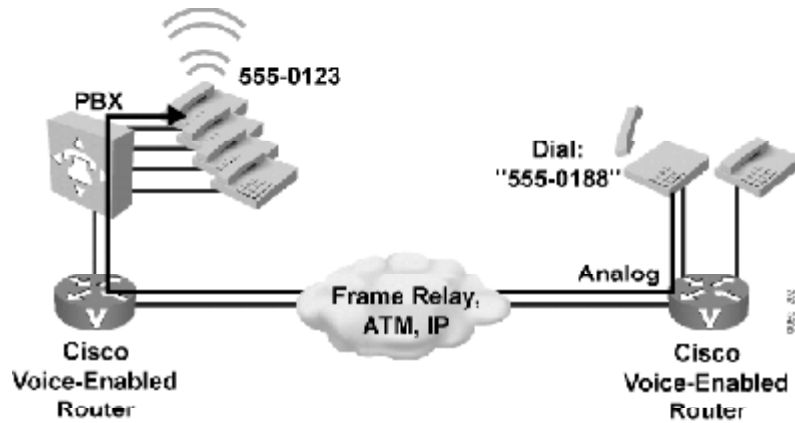
Voice Port Applications

Different types of applications require specific types of ports. In many instances, the type of port is dependent on the voice device that is connected to the network. This topic identifies the different types of voice port applications within the network.



In this example, local calls occur between two telephones connected to one Cisco voice-enabled router. This type of call is handled entirely by the router and does not travel over an external network. Both telephones are directly connected to Foreign Exchange Station (FXS) ports on the router.

On-Net Calls

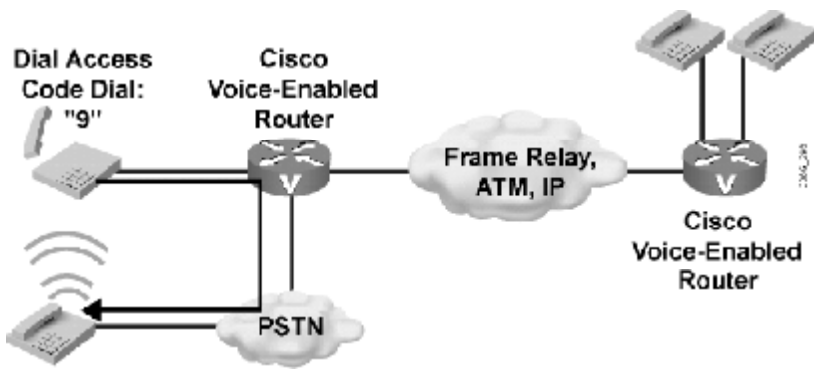


© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-2.4

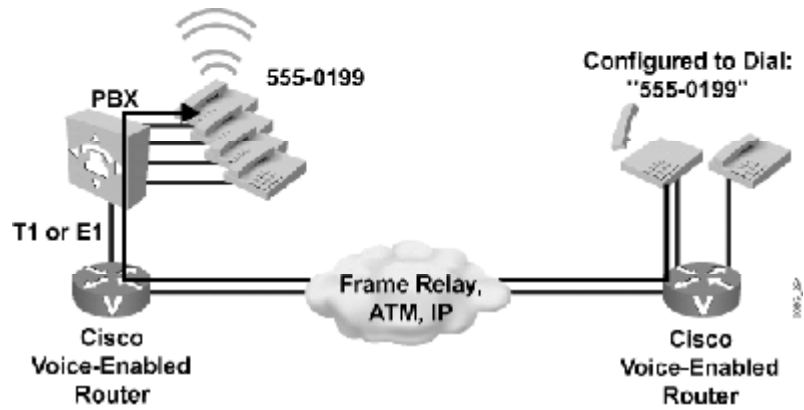
On-net calls occur between two telephones on the same data network. The calls can be routed through one or more Cisco voice-enabled routers, but the calls remain on the same data network. The edge telephones attach to the network through direct connections and FXS ports, or through a PBX, which typically connects to the network via a T1 connection. IP Phones that connect to the network via switches place on-net calls either independently or through the administration of Cisco CallManager. The connection across the data network can be a LAN connection, as in a campus environment, or a WAN connection, as in an enterprise environment.

Off-Net Calls



An off-net call occurs when a user dials an access code (such as “9”) from a telephone that is directly connected to a Cisco voice-enabled router or PBX to gain access to the public switched telephone network (PSTN). The connection to the PSTN is a single analog connection via a Foreign Exchange Office (FXO) port or a digital T1 or E1 connection.

PLAR

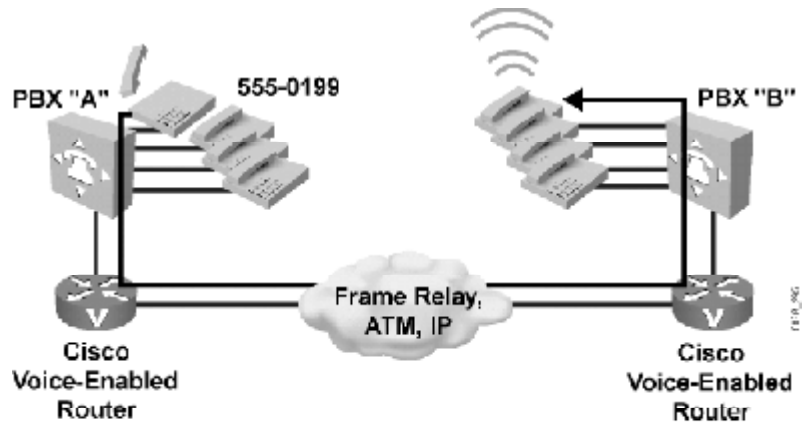


© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-2.6

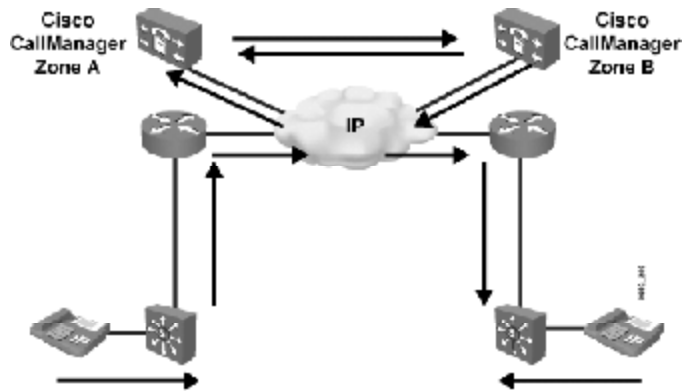
Private line, automatic ringdown (PLAR) calls automatically connect a telephone to a second telephone when the first telephone goes off hook. When this connection occurs, the user does not get a dial tone because the voice-enabled port for that telephone is preconfigured with a specific number to dial. A PLAR connection can work between any type of signaling, including E&M, FXO, FXS, or any combination of analog and digital interfaces.

PBX-to-PBX Calls



A PBX-to-PBX call originates at one PBX and terminates at another PBX while using the network for voice transport. Many business environments connect PBXs with private tie trunks. When migrating to a converged voice and data network, this same tie trunk connection can be emulated across the IP network. Modern PBX connections to the network are typically digital T1 or E1 with channel associated signaling (CAS) or PRI signaling. PBX connections may also be analog.

Cisco CallManager to Cisco CallManager

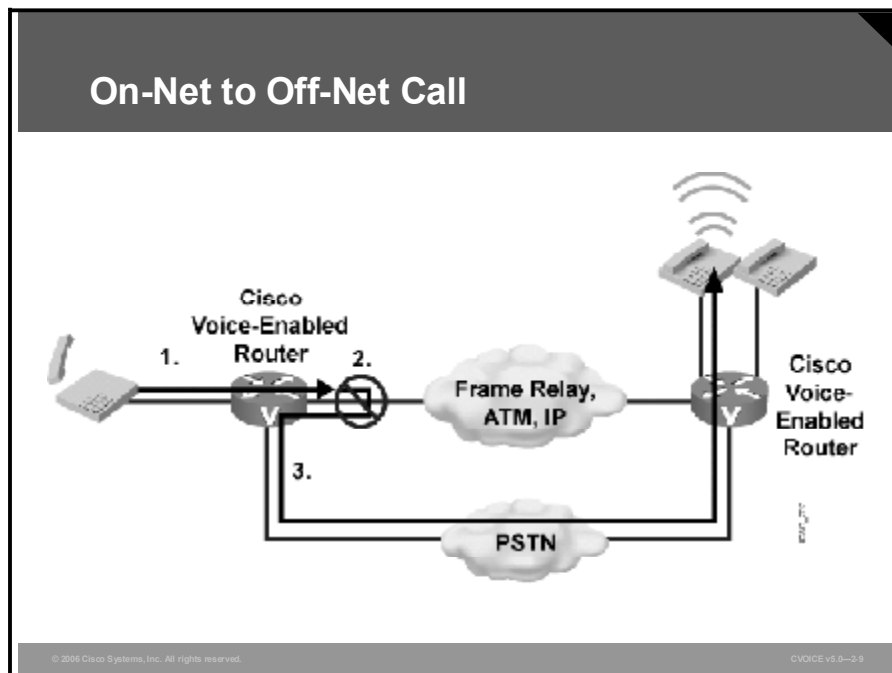


© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-2.8

As part of an overall migration strategy, a business may replace PBXs with Cisco CallManager. This includes IP Phones connected to the IP network. Cisco CallManager performs the call-routing functions formerly provided by the PBX. When an IP Phone call is placed using a configured Cisco CallManager, the call is assessed to see if the call is destined for another IP Phone under its control or if the call must be routed through a remote Cisco CallManager for call completion. Every Cisco CallManager is part of a zone. A zone is a collection of devices that are under a common administrator, which is usually a Cisco CallManager or gatekeeper. A call may stay on the IP network, even if it is sent between zones.

On-Net to Off-Net Call



A resilient call-routing strategy includes the ability to reroute calls through a secondary path should the primary path fail. On-net to off-net calls originate on an internal network and are routed to an external network (usually the PSTN). On-net to off-net call-switching functionality will be necessary when a network link is down or becomes overloaded and unable to handle the call volume presented.

Example: Voice Port Applications

The table lists application examples for each type of call.

Voice Port Call Types

Type of Call	Example
Local calls	One staff member calls another staff member at the same office. The call is switched between two ports on the same voice-enabled router.
On-net calls	One staff member calls another staff member at a remote office. The call is sent from the local voice-enabled router, across the IP network, and terminated on the remote office voice-enabled router.
Off-net calls	A staff member calls a client who is located in the same city. The call is sent from the local voice-enabled router that acts as a gateway to the PSTN. The call is then sent to the PSTN for call termination.
PLAR calls	A client picks up a customer service telephone located in the lobby of the office and is automatically connected to a customer service representative without dialing any digits. The call is automatically dialed, based on the PLAR configuration of the voice port. In this case, as soon as the handset goes off hook, the voice-enabled router generates the preconfigured digits to place the call.
PBX-to-PBX calls	One staff member calls another staff member at a remote office. The call is sent from the local PBX, through a voice-enabled router, across the IP network, through the remote voice-enabled router, and terminated on the remote office PBX.
Cisco CallManager to Cisco CallManager calls	One staff member calls another staff member at a remote office using an IP Phone. The call setup is handled by the Cisco CallManagers at each location. After the call is set up, the IP Phones generate IP packets that carry voice between sites.
On-net to off-net calls	One staff member calls another staff member at a remote office while the IP network is congested. When the originating voice-enabled router determines that it cannot terminate the call across the IP network, it sends the call to the PSTN with the appropriate dialed digits to terminate the call at the remote office via the PSTN network.

FXS Ports

FXS ports connect analog edge devices. This topic identifies the parameters that are configurable on the FXS port.

FXS Voice Port Configuration

- **signal**
- **cptone**
- **description**
- **ring frequency**
- **ring cadence**
- **disconnect-ack**
- **busyout**
- **station id name**
- **station id number**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE vs.0-2-10

In North America, the FXS port connection functions with default settings most of the time. The same cannot be said for other countries and continents. Remember, FXS ports look like switches to the edge devices that are connected to them. Therefore, the configuration of the FXS port should emulate the switch configuration of the local PSTN.

Example: When to Configure FXS Ports

An international company has offices in the United States and England. Each PSTN provides signaling that is standard for its own country. In the United States, the PSTN provides a dial tone that is different from the dial tone in England. The signals that ring incoming calls are different in England. Another instance where the default configuration might be changed is when the connection is a trunk to a PBX or key system. In each of these cases, the FXS port must be configured to match the settings of the device to which it is connected .

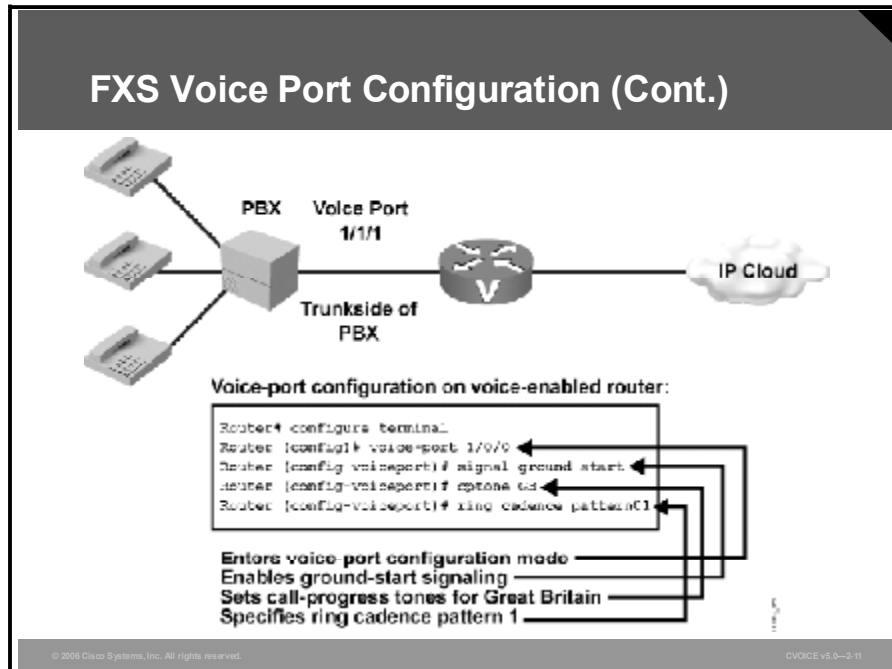
Configuration Parameters

FXS port configuration allows you to set parameters based on the requirements of the connection if default settings need to be altered or the parameters need to be set for fine-tuning. You can set these configuration parameters:

- **signal:** Sets the signaling type for the FXS port. In most cases, the default signaling of loop start works well. If the connected device is a PBX or a key system, the preferred signaling is ground start. Modern PBXs and key systems do not normally use FXS ports as connections to the network, but older systems may still have these interfaces. When connecting the FXS port to a PBX or key system, you must check the configuration of the voice system and set the FXS port to match it.
- **cptone:** Configures the appropriate call-progress tone for the local region. The call-progress tone setting determines the dial tone, busy tone, and ringback tone that the originating party hears.
- **description:** Configures a description for the voice port. You must use the description setting to describe the voice port in the **show** command output. It is always useful to provide some information about the usage of a port. The description might be used to specify the type of equipment that is connected to the FXS port.
- **ring frequency:** Configures a specific ring frequency (in hertz) for an FXS voice port. You must select the ring frequency that matches the connected equipment. If set incorrectly, the attached telephone might not ring or it might buzz. In addition, the ring frequency is usually country-dependent. You must consider the appropriate ring frequency for your area when you configure this command.
- **ring cadence:** Configures the ring cadence for an FXS port. The ring cadence defines how ringing voltage is sent to signal a call. The normal ring cadence in North America is 2 seconds of ringing followed by 4 seconds of silence. In England, normal ring cadence is a short ring followed by a longer ring. When configured, the **cptone** command automatically sets the ring cadence to match that country. You can manually set the ring cadence if you want to override the default country value. You may have to shut down and reactivate the voice port before the configured value takes effect.
- **disconnect-ack:** Configures an FXS voice port to remove line power if the equipment on an FXS loop-start trunk disconnects first. This removal of line power is not something the user hears, but instead is a method for electrical devices to signal that one side has ended the call.
- **busyout:** Configures the ability to busy out an analog port.
- **station id name:** Provides the station name associated with the voice port. This parameter is passed as a calling name to the remote end if the call is originated from this voice port. If no Caller ID is received on an FXO voice port, this parameter will be used as the calling name. Maximum string length is limited to 15.
- **station id number:** Provides the station number that is to be used as the calling number associated with the voice port. This parameter is optional. If it is configured, it will be used as the calling number of a call that is originated from this voice port. If it is not specified, the calling number will be used from a reverse dial-peer search. If no Caller ID is received on an FXO voice port, this parameter will be used as the calling number. Maximum string length is 15.

Example: FXS Port Configuration

This example shows how the British office is configured to enable ground-start signaling on a Cisco 2600 Series router or a Cisco 3600 Series out on FXS voice port 1/0/0. The call-progress tones are set for Great Britain, and the ring cadence is set for pattern 1.



FXO Ports

FXO ports act like telephones and connect to central office (CO) switches or to a station port on a PBX. This topic identifies the configuration parameters that are specific to FXO ports.

FXO Voice Port Configuration

- **signal**
- **ring number**
- **dial-type**
- **description**
- **supervisory disconnect**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2/12

Configuration Parameters

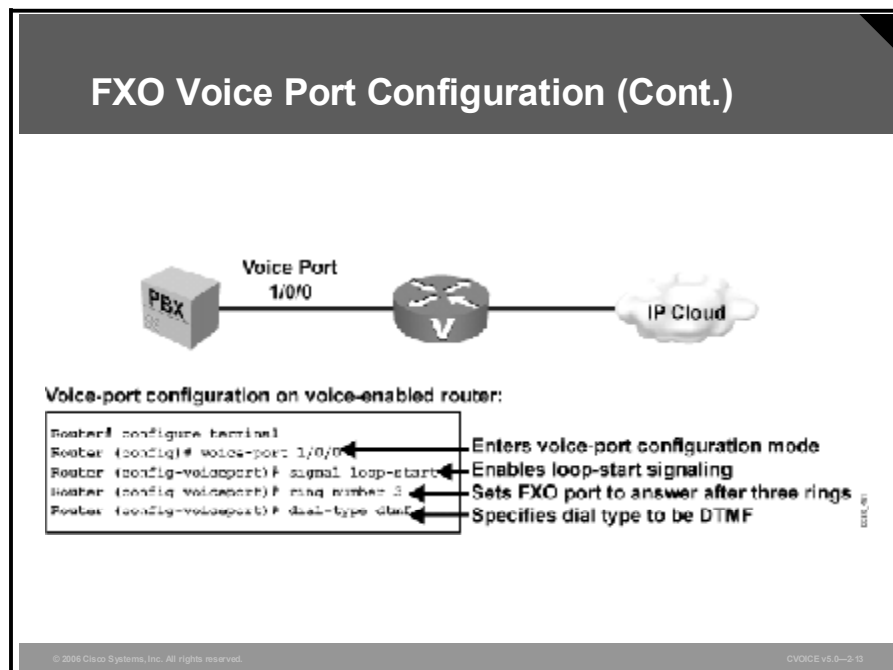
FXO port connections generally function with default settings. FXO port configuration allows parameters to be altered or fine-tuned based on the requirements of the connection. You can set these configuration parameters:

- **signal:** Sets the signaling type for the FXO port. If the FXO port is connected to the PSTN, the default settings are adequate. If the FXO port is connected to a PBX, the signal setting must match the PBX.
- **ring number:** Configures the number of rings before an FXO port answers a call. This is useful when you have other equipment available on the line to answer incoming calls. The FXO port answers if the equipment that is online does not answer the incoming call within the configured number of rings.
- **dial-type:** Configures the appropriate dial type for outbound dialing. Older PBXs or key sets may not support dual-tone multifrequency (DTMF) dialing. If you are connecting an FXO port to this type of device, you may need to set the dial type for pulse dialing.
- **description:** Configures a description for the voice port. Use the description setting to describe the voice port in the **show** command output.

- supervisory disconnect:** Configures supervisory disconnect signaling on the FXO port. Supervisory disconnect signaling is a power denial from the switch that lasts at least 350 ms. When this condition is detected, the system interprets this as a disconnect indication from the switch and clears the call. You should disable supervisory disconnect on the voice port if there is no supervisory disconnect available from the switch. Typically, supervisory disconnect is available when connecting to the PSTN and is enabled by default. When the connection extends out to a PBX, you should examine the documentation to ensure that supervisory disconnect is supported.

Example: FXO Port Configuration

The configuration in the figure enables loop-start signaling on a Cisco 2600 Series router or a Cisco 3600 Series router on FXO voice port 1/0/0. The ring-number setting of “3” specifies that the FXO port does not answer the call until after the third ring. The dial type is set to DTMF.



E&M Ports

E&M ports provide signaling that is generally used for switch-to-switch or switch-to-network trunk connections. This topic identifies the configuration parameters that are specific to the E&M port.

E&M Voice Port Configuration

- **signal**
- **operation**
- **type**
- **auto-cut-through**
- **description**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2-18

Configuration Parameters

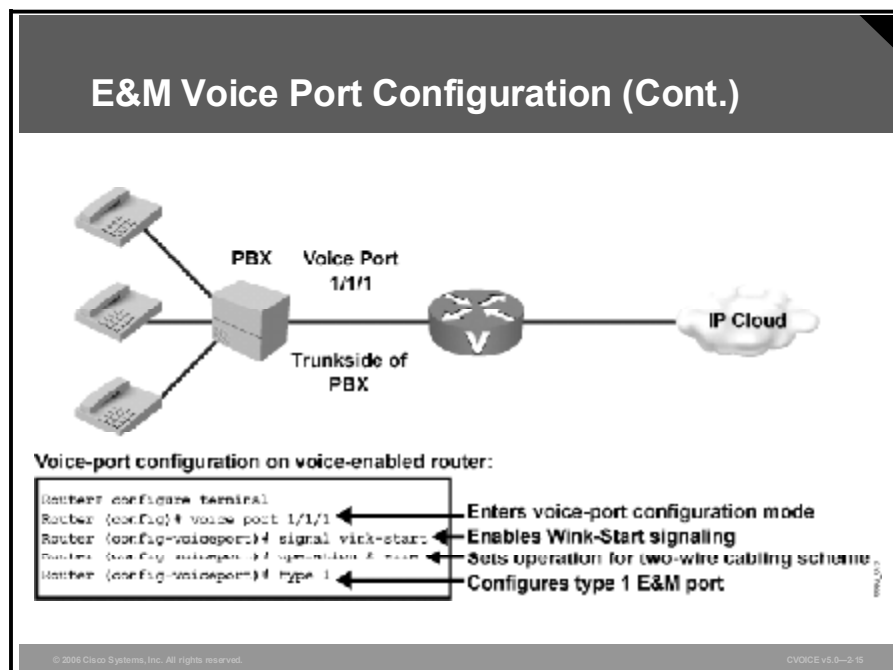
Although E&M ports have default parameters, you normally configure these parameters to match the device that is connected to the E&M port. You can set these configuration parameters:

- **signal:** Configures the signal type for E&M ports and defines the signaling that is used when notifying a port to send dialed digits. This configuration must match that of the PBX to which the port is connected. You must shut down and reactivate the voice port before the configured value takes effect.
 - With Wink-Start signaling, the router listens on the M-lead to determine when the PBX wants to place a call. When the router detects current on the M-lead, it waits for availability of digit registers and then provides a short wink on the E-lead to signal the PBX to start sending digits.
 - With delay start, the router provides current on the E-lead immediately upon seeing current on the M-lead. When current is stopped for the digit-sending duration, the E-lead stays high until digit registers are available.
 - With immediate start, the PBX simply waits a short time after raising the M-lead and then sends the digits without a signal from the router.

- **operation:** Configures the cabling scheme for E&M ports. The **operation** command affects the voice path only. The signaling path is independent of two-wire versus four-wire settings. If the wrong cable scheme is specified, the user may get voice traffic in one direction only. You must verify with the PBX configuration to ensure that the settings match. You must then shut down and reactivate the voice port for the new value to take effect.
- **type:** Configures the E&M interface type for a specific voice port. The type defines the electrical characteristics for the E-leads and M-leads. The E-leads and M-leads are monitored for on-hook and off-hook conditions. From a PBX perspective, when the PBX attempts to place a call, it goes high (off hook) on the M-lead. The switch monitors the M-lead and recognizes the request for service. If the switch attempts to pass a call to the PBX, the switch goes high on the E-lead. The PBX monitors the E-lead and recognizes the request for service by the switch. To ensure that the settings match, you must verify them with the PBX configuration.
- **auto-cut-through:** Configures the ability to enable call completion when a PBX does not provide an M-lead response. For example, when the router is placing a call to the PBX, even though they may have the same correct signaling configured, not all PBXs provide the wink with the same duration or voltage. The router may not understand the PBX wink. The **auto-cut-through** command allows the router to send digits to the PBX, even when the expected wink is not detected.
- **description:** Configures a description for the voice port. Use the **description** setting to describe the voice port in **show** command output.

Example: E&M Port Configuration

The configuration in the figure enables Wink-Start signaling on a Cisco 2600 Series router or a Cisco 3600 Series router on E&M voice port 1/1/1. The operation is set for the two-wire voice-cabling scheme, and the type is set to 1.



Timers and Timing

This topic identifies the timing requirements and adjustments that are applicable to voice interfaces. Under normal use, these timers do not need to be adjusted. There are two instances where these timers can be configured to allow more or less time for a specific function. One is when ports are connected to a device that does not properly respond to dialed digits or hookflash. The second instance is when the connected device provides automated dialing,

Timers and Timing Configuration

- **timeouts initial**
- **timeouts interdigit**
- **timeouts ringing**
- **timing digit**
- **timing interdigit**
- **timing hookflash-in and hookflash-out**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2-16

Configuration Parameters

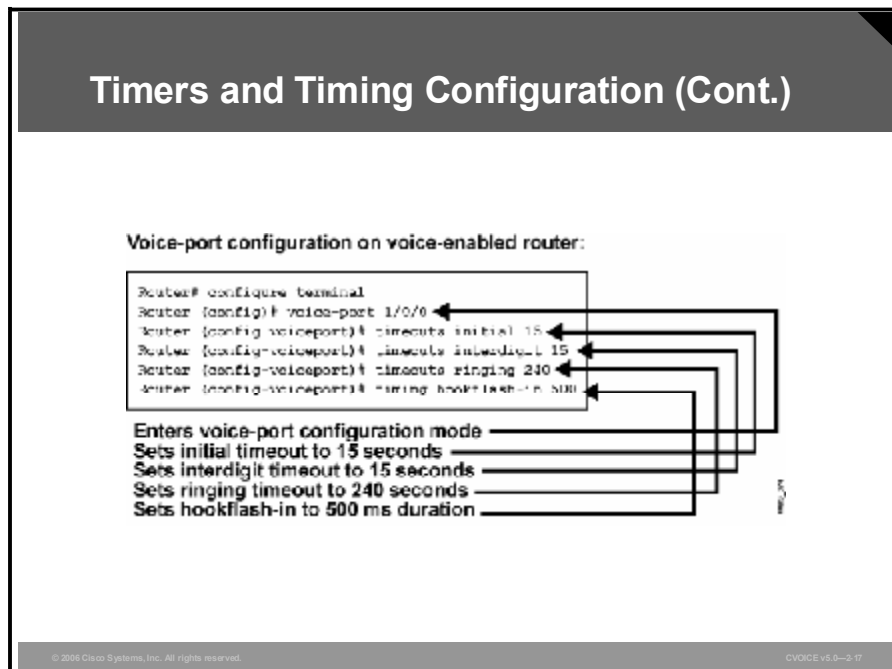
You can set a number of timers and timing parameters for fine-tuning the voice port. Here are voice port configuration parameters that you can set:

- **timeouts initial:** Configures the initial digit timeout value in seconds. This value controls how long the dial tone is presented before the first digit is expected. This timer value typically does not need to be changed.
- **timeouts interdigit:** Configures the number of seconds for which the system will wait between caller entered digits before sending the input to be assessed. If the digits are coming from an automated device, and the dial plan is a variable-length dial plan, you can shorten this timer so that the call proceeds without having to wait the full default of 10 seconds for the interdigit timer to expire.
- **timeouts ringing:** Configures the length of time that a caller may continue to let the telephone ring when there is no answer. You can configure this setting to be less than the default of 180 seconds, so that you do not tie up the voice port when it is evident that the call is not going to be answered.

- **timing digit:** Configures the DTMF digit signal duration for a specified voice port. You can use this setting to fine-tune a connection to a device that may have trouble recognizing dialed digits. If a user or device dials too quickly, the digit may not be recognized. By changing the timing on the digit timer, you can provide for a shorter or longer DTMF duration.
- **timing interdigit:** Configures the DTMF interdigit duration for a specified voice port. You can change this setting to accommodate faster or slower dialing characteristics.
- **timing hookflash-in and hookflash-out:** Configures the maximum duration (in milliseconds) of a hookflash indication. Hookflash is an indication by a caller that the caller wishes to do something specific with the call, such as transfer the call or place the call on hold. For the **hookflash-in** command, if the hookflash lasts longer than the specified limit, the FXS interface processes the indication as on hook. If you set the value too low, the hookflash may be interpreted as a hang up; if you set the value too high, the handset has to be left hung up for a longer period to clear the call. For the **hookflash-out** command, the setting specifies the duration (in milliseconds) of the hookflash indication that the gateway generates outbound. You can configure this to match the requirements of the connected device.

Example: Timers Configuration

The installation in the figure is for a home for the elderly, where users may need more time to dial digits than in other residences. Also, the requirement is to allow the telephone to ring, unanswered, for 4 minutes to allow more time for a resident to answer the telephone. The configuration in the figure enables several timing parameters on a Cisco voice-enabled router voice port 1/0/0. The initial timeout is lengthened to 15 seconds, the interdigit timeout is lengthened to 15 seconds, the ringing timeout is set to 240 seconds, and the **hookflash-in** is set to 500 ms.



Digital Voice Ports

This topic identifies the configuration parameters that are specific to T1 and E1 digital voice ports.

Basic T1/E1 Controller Configuration		
Command	T1	E1
framing	SF, ESF	CRC4, no-CRC4, Australia
linecode	AMI, B8ZS	AMI, HDB3
clock source	line, internal	line, internal

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2/15

Configuration Parameters

When you purchase a T1 or E1 connection, make sure that your service provider gives you the appropriate settings. Before you configure a T1 or E1 controller to support digital voice ports, you must enter the basic configuration parameters that follow to bring up the interface:

- **framing:** Selects the frame type for a T1 or E1 data line. The framing configuration differs between T1 and E1.
 - **Options for T1:** Super Frame (SF) or Extended Superframe (ESF)
 - **Options for E1:** 4-bit cyclic redundancy check (CRC4), no CRC4, or Australia
 - **Default for T1:** SF
 - **Default for E1:** CRC4
- **linecode:** Configures the line-encoding format for the digital service level 1 (DS1) link.
 - **Options for T1:** Alternate mark inversion (AMI) or binary 8-zero substitution (B8ZS)
 - **Options for E1:** AMI or high density binary 3 (HDB3)
 - **Default for T1:** AMI
 - **Default for E1:** HDB3
- **clock source:** Configures clocking for individual T1 or E1 links.
 - **Options:** Line or internal
 - **Default:** Line

T1/E1 Digital Voice Configuration

Create digital voice ports with the `ds0-group` command:

- `ds0-group-no`
- `timeslot-list`
- `signal-type`

You must create a digital voice port in the T1 or controller to be able to configure voice port parameters. You must also assign timeslots and signaling to the logical voice port through configuration. The first step is to create the T1 or E1 digital voice port with the **`ds0-group ds0-group-no timeslots timeslot-list type signal-type`** command.

The **`ds0-group`** command automatically creates a logical voice port that is numbered as `slot/port:ds0-group-no`.

The `ds0-group-no` argument identifies the digital signal zero (DS0) group (number from 0 to 23 for T1 and from 0 to 30 for E1). This group number is used as part of the logical voice port numbering scheme.

The **`timeslots`** command allows the user to specify which timeslots are part of the DS0 group. The `timeslot-list` argument is a single timeslot number, a single range of numbers, or multiple ranges of numbers separated by commas.

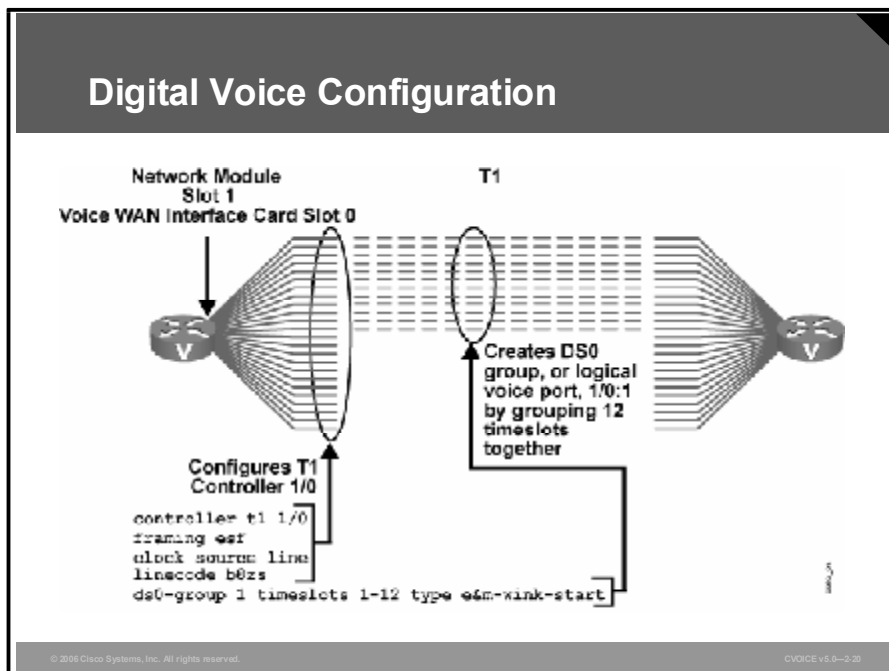
The **`type`** command defines the emulated analog signaling method that the router uses to connect to the PBX or PSTN. The type depends on whether the interface is T1 or E1.

When you specify a **`ds0-group`** command, the system creates a logical voice port. You must then enter the voice-port configuration mode to configure port-specific parameters. To enter voice-port configuration mode on Cisco 2600 Series multiservice platforms or Cisco 3600 Series multiservice platforms, use the **`voice-port slot/port:ds0-group-no`** command.

To delete a DS0 group, you must first shut down the logical voice port. When the port is in shutdown state, you can remove the DS0 group from the T1 or E1 controller with the **`no ds0-group ds0-group-no`** command.

Example: T1 Configuration

This example configures the T1 controller for ESF, B8ZS line code, and timeslots 1 through 12 with E&M Wink-Start signaling. The resulting logical voice port is 1/0:1, where 1/0 is the module and slot number and :1 is the *ds0-group-no* argument that was assigned during configuration. You can configure the remaining timeslots for other signaling types or leave them unused.



ISDN

This topic identifies ISDN configurations for voice ports.

ISDN Configuration

- **Global configuration**
 - **isdn switch-type**
- **T1/E1 controller configuration**
 - **pri-group**
- **D-channel configuration**
 - **isdn incoming-voice configuration**
- **QSIG configuration**
 - **QSIG signaling**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0-2.21

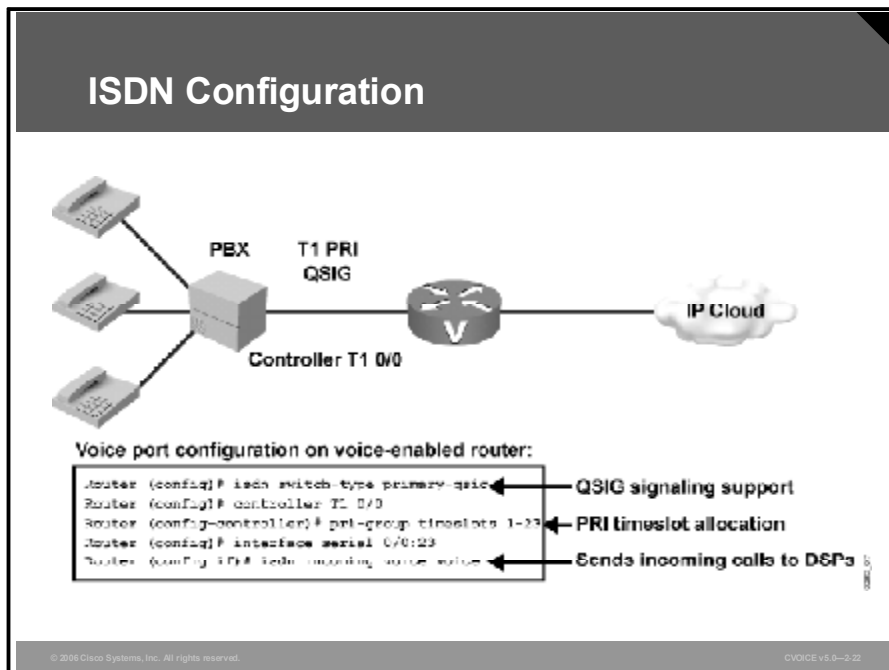
Configuration Parameters

Cisco voice-capable devices provide support for both PRI and BRI voice connections. Many PBX vendors support either T1/E1 PRI or BRI connections. In Europe, where ISDN is more popular, many PBX vendors support BRI connections. When designing how the PBX passes voice to the network, you must ensure that the router supports the correct connection. The first step in provisioning ISDN capabilities for T1 or E1 PRI is to enter the basic configuration of the controllers. After the clock source, framing, and line code are configured, ISDN voice functionality requires these configuration commands:

- **isdn switch-type:** Configures the ISDN switch type. You can enter this parameter in global configuration mode or at the interface level. If you configure both, the interface switch type takes precedence over the global switch type. This parameter must match the provider ISDN switch. This setting is required for both BRI and PRI connections.
- **pri-group:** Configures timeslots for the ISDN PRI group. T1 allows for timeslots 1 to 23, with timeslot 24 allocated to the data channel (D channel). E1 allows for timeslots 1 to 31, with timeslot 16 allocated to the D channel. You can configure the PRI group to include all available timeslots, or you can configure only a select group of timeslots.
- **isdn incoming-voice:** Configures the interface to send all incoming calls to the digital signal processor (DSP) card for processing.
- **QSIG signaling:** Configures the use of Q Signaling (QSIG) signaling on the D channel. You typically use this setting when connecting via ISDN to a PBX. The command to enable QSIG signaling is **isdn switch-type primary-qsig** for PRI and **isdn switch-type basic-qsig** for BRI connections.

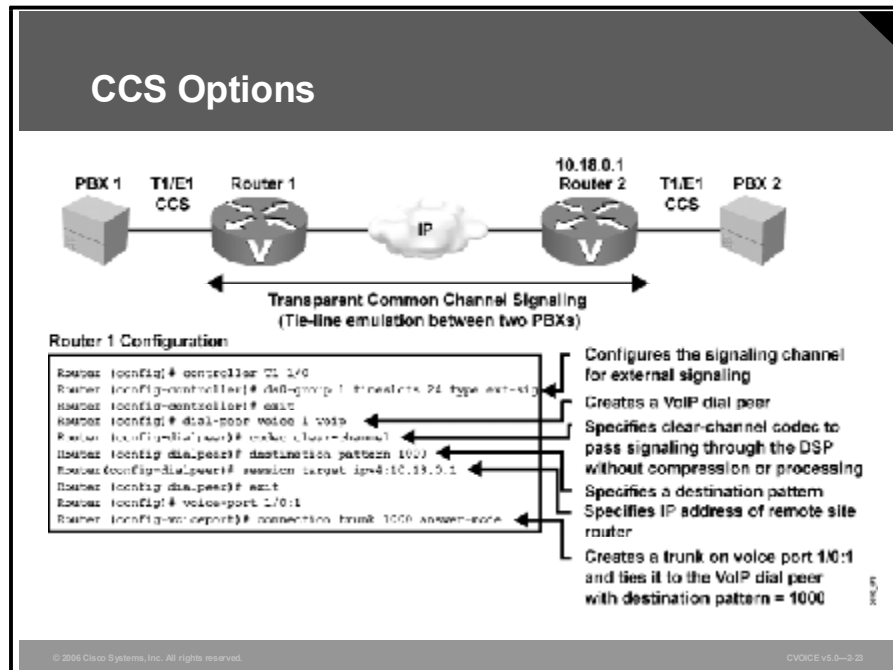
Example: ISDN QSIG Configuration

This example shows the configuration for a PBX connection to the Cisco voice-enabled router. The connection is configured for QSIG signaling across all 23 timeslots.



CCS Options

This topic describes how to pass proprietary signaling between two PBXs through the use of Transparent Common Channel Signaling (T-CCS).



In many cases, PBXs support proprietary signaling that is used to signal supplementary services only, such as making a light on the telephone blink when voice mail is waiting. Because the router does not understand this proprietary signaling, the signaling must be carried transparently across the network without interpretation. T-CCS allows the connection of two PBXs with digital interfaces that use a proprietary or unsupported common channel signaling (CCS) protocol. T1 and E1 traffic is transported transparently through the data network, and the T-CCS feature preserves proprietary signaling. From the PBX standpoint, this type of communication is accomplished through a point-to-point connection. Calls from the PBXs are not routed, but they do follow a preconfigured route to the destination.

T-CCS Configuration Process

The configuration for T-CCS in a Voice over IP (VoIP) environment calls for this three-step process:

Step 1 Define the DS0 group.

Configure the command **ds0-group** *ds0-group-no timeslots timeslot-list type ext-sig* in the T1 or E1 controller configuration mode. The **timeslots** command specifies the D channel that carries call signaling. The **type ext-sig** command specifies that the signaling is coming from an external source.

Step 2 Create the dial peer.

- Configure a VoIP dial peer that points to the IP address of the remote voice-enabled router that connects to the remote PBX.
- Configure the dial peer for the clear-channel codec that signals the DSP to pass the signaling without interpretation.
- The destination pattern specified in this dial peer is used to create a trunk in Step 3. The number entered here must match the number entered in the **trunk** command.
- The session target specifies the IP address of the remote voice-enabled router.
- Configure the dial peer to point to the IP address of the remote site voice-enabled router using the **session target** command.

Step 3 Create the voice port trunk.

Configure the **connection trunk** *digits answer-mode* command at the logical voice port to create a trunk from that port through the VoIP dial peer and across the IP network to the remote router. The *digits* parameter must match the destination pattern in the VoIP dial peer created in Step 2. The **answer-mode** parameter specifies that the router should not attempt to initiate a trunk connection but should wait for an incoming call before establishing the trunk.

The process for passing the signal transparently through the IP network is as follows:

Step 1 PBX 1 sends proprietary signaling across the signaling channel to router 1.

Step 2 The logical voice port that corresponds to the signaling channel is configured for trunking. This causes the router to look for the dial peer that matches the **trunk** *digits* parameter.

Step 3 The VoIP dial peer is configured for the clear-channel codec and points to the IP address of the remote router (router 2) connecting the remote PBX (PBX 2).

Step 4 The remote router has a plain old telephone service (POTS) dial peer configured that points to the logical voice port that is associated with the signaling channel of PBX 2. The signal arrives at PBX 2 in its native form.

This process shows the T-CCS signaling part of the configuration only. Additional DS0 group and dial-peer configuration is necessary for transport of the voice channels.

Monitoring and Troubleshooting

This topic describes the **show**, **test** and **debug** commands that are used to monitor and troubleshoot voice ports.

Verifying and Troubleshooting Voice Ports

1. **Check for dial tone (FXS only).**
2. **Check for DTMF tones (FXS only).**
3. **Use the show voice port command to check the configuration.**
4. **Use the show voice port command to ensure that the port is enabled.**
5. **Be sure that the PBX configuration is compatible with the voice port.**
6. **Check the physical installation of the hardware.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE vs.0-2.34

You can perform these steps to verify voice port configuration:

- Step 1** Pick up the handset of an attached telephony device and check for a dial tone. If there is no dial tone, check the following:
- Is the plug firmly seated?
 - Is the voice port enabled?
 - Is the voice port recognized by the Cisco IOS software?
 - Is the router running the correct version of Cisco IOS software to recognize the module?
- Step 2** If you have a dial tone, check for DTMF voice band tones, such as touch-tone detection. If the dial tone stops when you dial a digit, the voice port is probably configured properly.
- Step 3** Use the **show voice port** command to verify that the configuration is correct. If you have trouble connecting a call, and you suspect that the problem is associated with voice port configuration, you can try to resolve the problem by performing Step 4 through Step 6.
- Step 4** Use the **show voice port** command to make sure that the port is enabled. If the port is administratively down, use the **no shutdown** command. If the port was working previously and is not working now, it is possible that the port is in a hung state. Use the **shutdown/no shutdown** command sequence to reinitialize the port.

- Step 5** If you have configured E&M interfaces, make sure that the values associated with your specific PBX are correct. Check for two-wire or four-wire Wink-Start, immediate-start, or delay-start signaling types, and the E&M interface type. These parameters need to match those set on the PBX for the interface to communicate properly.
- Step 6** You must confirm that the voice network module (VNM) is correctly installed. With the device powered down, remove the VNM and reinsert it to verify the installation. If the device has other slots available, try inserting the VNM into another slot to isolate the problem. Similarly, you must move the voice interface card (VIC) to another VIC slot to determine if the problem is with the VIC or with the module slot.

Commands to Verify Voice Ports

Command	Description
<code>show voice port</code>	Shows all voice port configurations in detail
<code>show voice port x/y/z</code>	Shows one voice port configuration in detail
<code>show voice port summary</code>	Shows all voice port configurations in brief
<code>show voice busyout</code>	Shows all ports configured as busyout
<code>show voice dsp</code>	Shows all DSP statuses
<code>show controller T. 0/1</code>	Shows the operational status of the controller

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2.25

There are six **show** commands for verifying the voice port and dial-peer configuration. These commands and their functions are shown in the figure.

Test Commands

Command	Description
<code>test voice port detector {in load battery-reversal ringer ring-ground ring-trap} {on off disable}</code>	This command forces a detector into specific states for testing. For each signaling type (E&M, FXO, FXS), only the applicable keywords display.
<code>test voice port inject-tone {line1 network} {1000Hz 2000Hz 3000Hz 1000Hz 2000Hz 3000Hz 500Hz quiet disable}</code>	This command injects a test tone into a voice port. A call must be established on the voice port under test. When you are finished testing, be sure to enter the <code>disable</code> command to end the test tone.
<code>test voice port loopback {local network disable}</code>	This command performs loopback testing on a voice port. A call must be established on the voice port under test.
<code>test voice port relay {E load loop ring-reversal battery-reversal power-down ring ring-ground} {on off disable}</code>	This command tests relay-related functions on a voice port.
<code>test voice port switch {fax disable}</code>	This command forces a voice port into fax or voice mode for testing. If the voice port does not detect fax data, the voice port remains in fax mode for 30 seconds and then reverts automatically to voice mode.
<code>csim xxxx</code>	This command simulates a call to destination <code>xxxx</code> .

The **test** commands provide the ability to analyze and troubleshoot voice ports on the Cisco 2600 Series routers and the Cisco 3600 Series routers. There are five **test** commands to force voice ports into specific states to test the voice port configuration.

When you finish the loopback testing, be sure to enter the **disable** command to end the forced loopback.

After you enter the **test voice port switch fax** command, you can use the **show voice call** command to check whether the voice port is able to operate in fax mode.

The **csim** command simulates a call to any end station for testing purposes. It is most useful when testing dial plans.

Note Refer to the *Voice Port Testing Enhancements in Cisco 2600 and 3600 Series Routers and MC3810 Series Concentrators* document for further information.
http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080024.html

ISDN Commands

Command	Description
show isdn active	Shows ISDN active calls
show isdn history	Shows ISDN call history
show isdn status	Shows ISDN line status
show isdn timers	Shows ISDN timer values
debug isdn events	Displays ISDN events
debug isdn q921	Displays ISDN Q.921 packet history
debug isdn q931	Displays ISDN Q.931 packet history

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-2.27

The ISDN **show** and **debug** commands in the figure are useful for viewing and troubleshooting ISDN connections.

Summary

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

Summary

- **Voice port applications include local, on-net, off-net, PLAR, PBX to PBX, Cisco CallManager to Cisco CallManager, and on-net to off-net calls.**
- **Configurable parameters on FXS ports include *signal, cptone, description, ring frequency, ring cadence, disconnect-ack, busyout, station id name, and station id number.***
- **Configurable parameters on FXO ports include *signal, ring number, dial-type, description, and supervisory disconnect.***
- **Configurable parameters on E&M ports include *signal, operation, type, auto-cut-through, and description.***

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-2.28

Summary (Cont.)

- **Configurable timer and timing parameters define initial digit and interdigit timing, digit and interdigit duration, and ringing time.**
- **Digital voice ports are created with the ds0-group command in the T1/E1 controller.**
- **ISDN configuration requires that the pri-group command specify timeslots used for voice and signaling.**
- **T-CCS allows for the transparent passing of proprietary PBX signaling across the IP network.**
- **The show, debug, and test commands are used for monitoring and troubleshooting voice functions in the network.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-2.28

References

For additional information, refer to these resources:

- *Configuring Voice Ports.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/voice_c/vcprt1/vcports.htm.
- *Configuring and Troubleshooting Transparent CCS.*
http://www.cisco.com/warp/public/788/voip/trans_channel_signal.html.
- *Configuring Voice Ports.*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvfax_c/vvfp0rt.htm

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 2-1: Connecting a Voice-Enabled Router

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) Match the type of voice application with its description.
- A) local call
 - B) on-net call
 - C) off-net call
 - D) on-net to off-net call
- _____ 1. a type of call for which the user dials an access code to connect to the PSTN
- _____ 2. a type of call that is handled entirely by one router and does not go across an external network
- _____ 3. a type of call that is rerouted through a secondary path when the primary path fails
- _____ 4. a type of call that may be routed through one or more routers, but stays on the same network
- Q2) If a client picked up a customer service handset and was automatically connected to customer service without dialing any digits, what kind of call would it be?
- A) Cisco CallManager to Cisco CallManager call
 - B) PBX-to-PBX call
 - C) on-net call
 - D) local call
 - E) PLAR call
- Q3) Which configuration parameter would you change to set the dial tone, busy tone, and ringback tone?
- A) **cptone**
 - B) **ring frequency**
 - C) **ring cadence**
 - D) **description**
 - E) **signal**
- Q4) Which situations most likely require changes to the FXS port default settings?
- A) The caller and the called party are in different parts of the country.
 - B) The caller and the called party are in different countries.
 - C) The connection is a trunk to a PBX.
 - D) The FXS port configuration does not match the local PSTN switch configuration.
- Q5) Which description best describes supervisory disconnect signaling?
- A) a power denial from the switch that lasts at least 350 ms
 - B) a disconnect message manually sent by the network administrator
 - C) signaling used by the main voice port of the PBX switch
 - D) a disconnect process overseen by the network administrator

- Q6) When connecting an FXO port to a device that supports pulse dialing, which command is optional?
- A) **signal**
 - B) **dial-type**
 - C) **description**
 - D) **supervisory disconnect**
- Q7) The wrong cable scheme is specified during E&M port configuration. What is the likely outcome?
- A) The signal will not be transmitted.
 - B) The voice traffic will go in one direction only.
 - C) The voice ports will not be activated.
 - D) The switch will not recognize a request for service.
- Q8) A router provides current on the E-lead as soon as it sees current on the M-lead. What type of signaling is being used?
- A) delay-start signaling
 - B) immediate-start signaling
 - C) Wink-Start signaling
 - D) QSIG
- Q9) It is desired to set a limit on the number of seconds to wait between dialed digits before digit input evaluation. Which parameter should be configured?
- A) **timeouts initial**
 - B) **timeouts interdigit**
 - C) **timing digit**
 - D) **timing interdigit**
- Q10) What is the default setting for the **timeouts ringing** configuration parameter?
- A) 15 seconds
 - B) 60 seconds
 - C) 100 seconds
 - D) 180 seconds
- Q11) What are the two options for the **framing** command on a T1 connection? (Choose two.)
- A) SF
 - B) ESF
 - C) CRC4
 - D) AMI
 - E) B8ZS
 - F) HDB3
- Q12) What are the two options for the **linecode** command on an E1 connection? (Choose two.)
- A) SF
 - B) ESF
 - C) CRC4
 - D) AMI
 - E) B8ZS
 - F) HDB3

- Q13) For E1 connections, which timeslot is allocated to the D channel?
- A) 1
 - B) 16
 - C) 23
 - D) 31
- Q14) Which configuration command is required for ISDN voice functionality?
- A) **dial-type**
 - B) **disconnect-ack**
 - C) **busyout**
 - D) **pri-group**
 - E) **ds0-group**
- Q15) What is the purpose of T-CCS?
- A) to route calls between PBXs
 - B) to provide point-to-point connections between PBXs
 - C) to pass proprietary signaling between PBXs
 - D) to specify a channel for call signaling
- Q16) The **trunk number** entered in configuring T-CSS in a VoIP network must match the **trunk number** entered in which command?
- A) **timeslots**
 - B) **dial-peer**
 - C) **destination-pattern**
 - D) **session target**
- Q17) After you enter the **test voice port switch fax** command, which command can you use to check whether the voice port can operate in fax mode?
- A) **show voice port**
 - B) **show voice call**
 - C) **show fax port**
 - D) **show switch call**
 - E) **show fax call**
- Q18) Which two conditions can be checked by using the **show voice port** command? (Choose two.)
- A) The data that is configured is correct.
 - B) The port is enabled.
 - C) The E&M interfaces are configured correctly.
 - D) The PBX setup values are correct.

Lesson Self-Check Answer Key

- Q1) 1-C, 2-A, 3-D, 4-B
Relates to: Voice Port Applications
- Q2) E
Relates to: Voice Port Applications
- Q3) A
Relates to: FXS Ports
- Q4) B
Relates to: FXS Ports
- Q5) A
Relates to: FXO Ports
- Q6) B
Relates to: FXO Ports
- Q7) B
Relates to: E&M Ports
- Q8) B
Relates to: E&M Ports
- Q9) B
Relates to: Timers and Timing
- Q10) D
Relates to: Timers and Timing
- Q11) A, B
Relates to: Digital Voice Ports
- Q12) D, F
Relates to: Digital Voice Ports
- Q13) B
Relates to: ISDN
- Q14) D
Relates to: ISDN
- Q15) C
Relates to: CCS Options
- Q16) C
Relates to: CCS Options

Q17) B
Relates to: Monitoring and Troubleshooting

Q18) A, B
Relates to: Monitoring and Troubleshooting

Lesson 2

Adjusting Voice Interface Settings

Overview

Voice interface settings affect voice quality. There are a number of settings that you can configure to enhance the quality of voice traffic on voice ports.

Relevance

User acceptance of the converged voice and data network depends on the quality of current calls compared to the quality experienced through their original providers. As new devices are introduced into the voice path, it is important to understand how the electrical characteristics of interfaces impact voice quality. This lesson discusses these electrical characteristics and how to fine-tune them for improved voice quality.

Objectives

Upon completing this lesson, you will be able to configure analog and digital voice ports for optimal voice quality. This ability includes being able to meet these objectives:

- Describe the electrical characteristics of analog voice and the factors affecting voice quality
- Assess and configure required input and output power levels
- Configure voice port parameters to fine-tune voice quality
- Configure echo cancellation on the voice ports to improve voice quality

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Familiarity with Cisco IOS configuration modes
- Familiarity with analog and digital voice port usage

Outline

The outline lists the topics included in this lesson.

Outline

- **Overview**
- **Factors Affecting Voice Quality**
- **Setting Input and Output Power Levels**
- **Voice Quality Tuning**
- **Echo Cancellation Commands**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2.2

Factors Affecting Voice Quality

This topic describes the electrical characteristics of analog voice and the factors affecting voice quality.

Factors Affecting Voice Quality

These factors affect voice quality:

- **Transmit and receive power levels**
- **Input gain**
- **Output attenuation**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2-3

Voice signal power in a long-distance connection must be tightly controlled. The delivered signal power must be high enough to be clearly understood, but not so strong that it leads to instabilities such as echo. In the traditional telephony network, telephone companies control the signal power levels at each analog device. Now that the IP network is carrying voice, it may be necessary to adjust signal power on a voice interface to fine-tune the voice quality.

Most initial voice signals enter the network through a two-wire local loop. Most switches connect to other switches through a four-wire connection. As voice travels through the network for delivery to the remote telephone, the voice signal must be passed from the two-wire local loop to the four-wire connection at the first switch, then from the four-wire connection at the switch to a two-wire local loop at the remote end. If the impedance at these two-wire to four-wire connections is not matched exactly, some of the voice signal reflects back in the direction of the source. As a result, originating callers hear their own voice reflected back. Sometimes, the reflected signal is reflected again, causing the destination to hear the same conversation twice.

In a traditional voice network, voice can reflect back; it usually goes unnoticed, however, because the delay is so low. In a Voice over IP (VoIP) network, echo is more noticeable because both packetization and compression contribute to delay.

Another problem is inconsistent volume at different points in the network. Both echo and volume inconsistency may be caused by a voice port that is generating a signal level that is too high or too low. You can adjust signal strength in the inbound direction from an edge telephone or switch into the voice port and in the outbound direction from the voice port to the edge telephone or switch. Echo results from incorrect input or output levels or from an impedance mismatch. Impedance value must match the setting from the specific telephony system to which it is connected. Mismatched impedance values produce echo in the voice path. Although these adjustments are available on the Cisco voice equipment, they are also adjustable on PBX equipment.

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 become distorted at a very low volume and dual tone multifrequency (DTMF) may be missed.

Setting Input and Output Power Levels

Change in signal strength is measured in decibels (dBs). You can either boost the signal or attenuate it by configuring the voice port for input gain or output attenuation. You must be aware of what a voice port connects to and know at what decibel level that device works best. This topic describes how to calculate and baseline input and output power levels.

Calculating network decibel levels is often an exercise in simple number line arithmetic. The table provides common decibel levels.

Calculating Decibel Levels						
Source 1 Out/In	Router 1 Adjustment	Net at Router 1	WAN	Net at M Router 2	Router 2 Adjustment	Destination 1 In/Out
0 dB →	-3 dB →	-3 dB	—	-3 dB	±6 dB →	→ -9 dB
-9 dB ←	← ±6 dB	-3 dB	—	-3 dB	-3 dB	← -0 dB

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2-4

Baselining Input and Output Power Levels

Considerations for baselining input and output power levels are as follows:

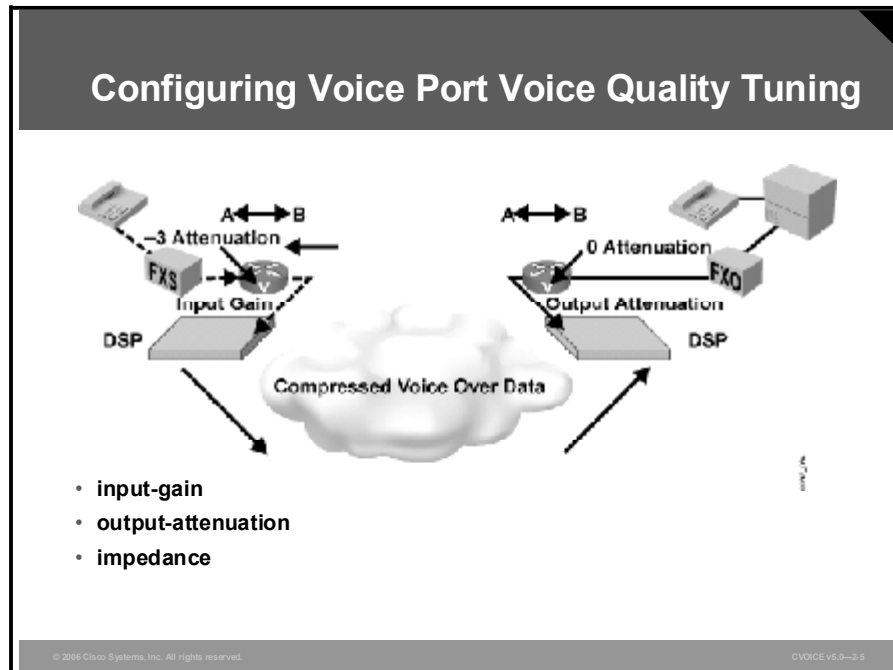
- Analog voice routers operate best when the receive level from an analog source is set at approximately -3 dB.
- In the United States and most of Europe, the receive (transmit) level that is normally expected for an analog telephone is approximately -9 dB. In Asian and South American countries, receive levels are closer to -14 dB. To accommodate these differences, the output levels to the router are set over a wide range.
- Overdriving the circuit can cause analog clipping. Clipping occurs when the power level is above available pulse code modulation (PCM) codes, and a continuous repetition of the last PCM value is passed to the digital signal processor (DSP).
- Echo occurs when impedance mismatches reflect power back to the source.

Example: Decibel Levels

Adjustment of decibel levels may be necessary throughout a voice network. A station connected to a PBX may experience one level of loudness when calling a local extension, a different level when dialing an outside line, and different levels when calling remote sites via VoIP. Adjustments will be necessary in this case.

Voice Quality Tuning

This topic describes voice-quality tuning configuration.



In an untuned network, a port configuration that delivers perceived good quality for a call between two dial peers might deliver perceived poor quality for a call between two other dial peers.

Voice quality adjustment is a defined, step-by-step procedure that is implemented after the network is up and running. It is ineffective for you to begin changing the default voice port configurations until full cross-network calls are established. A correctly implemented procedure will result in a quality compromise between various sources that the customer accepts as good overall quality.

A variety of different factors, including input gain and output attenuation, can affect voice quality.

A loss plan looks at the required decibel levels at specific interfaces, such as an analog Foreign Exchange Station (FXS) port connecting to a telephone, or a Foreign Exchange Office (FXO) port connecting to the public switched telephone network (PSTN). An analog voice router works best with a receive level of -3 dB. An analog telephone in North America and Europe works best with a receive level of -9 dB. Therefore, if the device connecting to that router provides a different level than the expected -3 dB, input gain can be set to equalize it to -3 dB. If the output at the other end is a telephone that expects -9 dB, the output voice port has to provide -6 dB output attenuation in addition to the -3 dB to send signaling to the telephone at the expected -9 dB levels. A systemwide loss plan looks at the decibel levels of the initial input and the remote output ports and plans for the appropriate adjustments for end-to-end signal levels. You must consider other equipment (including PBXs) in the system when creating a loss plan.

Configuration Parameters

Parameters for configuring voice port voice quality tuning are as follows:

- **input-gain:** Configures a specific input gain, in decibels, to insert into the receiver side of the interface. The default value for this command assumes that a standard transmission loss plan is in effect, meaning that there must be an attenuation of -6 dB between telephones. The standard transmission plan defines country-specific decibel levels and assumes that interfaces already provide the expected decibel levels. For example, there must be attenuation of -6 dB between two telephones so that the input gain and output attenuation is 0 if the interfaces provide the required -6 dB attenuation.

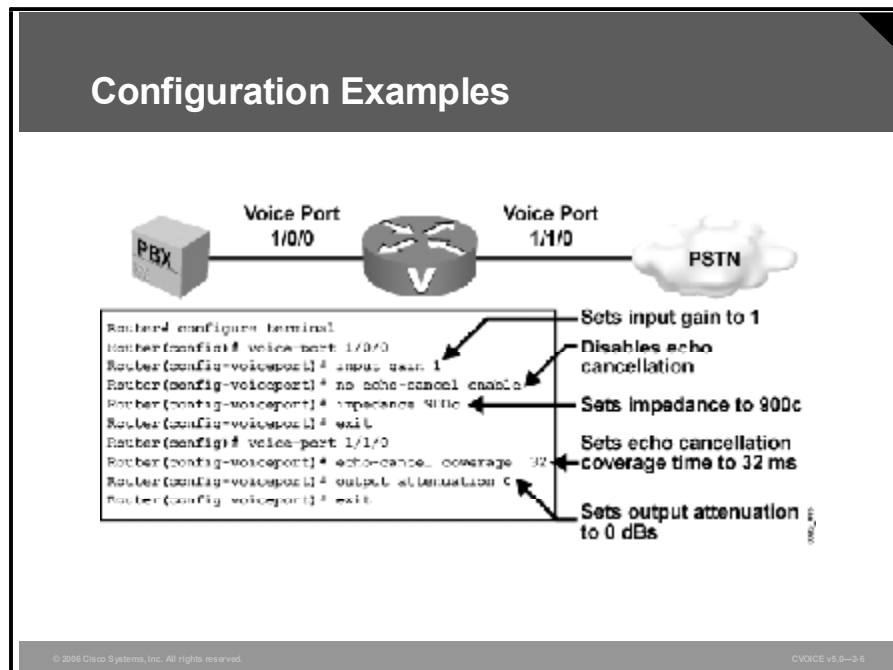
The gain of a signal to the PSTN can only be decreased. The gain of a signal coming into the router can be increased.

- **output-attenuation:** Configures the output attenuation value in decibels for the transmit side. The value represents the amount of loss to be inserted at the transmit side of the interface.
- **impedance:** Configures the terminating impedance of a voice port interface. The impedance value that is selected must match the setting from the specific telephony system to which it is connected. You must verify the impedance settings in the technical specifications document of the device. Impedance standards vary between countries. Central office (CO) switches in the United States are predominantly 600 ohms real (600r). PBXs in the United States are normally 600r or 900 ohms complex (900c).

Incorrect impedance settings or an impedance mismatch generates a significant amount of echo. You can mask the echo by enabling the **echo-cancel** command. Gains often do not work correctly if there is an impedance mismatch.

Note The **input-gain** and **output-attenuation** commands accommodate network equipment and are not end-user volume controls for user comfort.

Example: Voice Port Tuning



This example shows voice port tuning parameters on the E&M and FXO ports of a Cisco voice-enabled router. In the example, the PBX output is -4 dB, whereas the voice router functions best at -3 dB. Therefore, the adjustment is made in the inbound path to the router using the **input-gain** command. The impedance setting on the router needs to be changed from the default of 600 Ω to match the 900 Ω impedance setting for the PBX. Because this is an E&M port, echo cancellation is disabled. The FXO port connecting to the PSTN has an adjustment for echo coverage that allows for longer-distance echo cancellation.

Here are some of the E&M voice port parameters:

- **input-gain:** Increases the inbound voice level by 1 dB before the voice is transmitted across the network
- **no echo-cancel enable:** Disables echo cancellation
- **impedance:** Sets the impedance to match the connecting hardware

Here are some of the FXO voice port parameters:

- **echo-cancel coverage:** Adjusts the cancellation coverage time to 32 ms. This allows for cancellation of echo that has greater delay.
- **output-attenuation:** Specifies that there is no attenuation as the signal is passed out of the interface to the PSTN.

Echo Cancellation Commands

This topic describes echo cancellation configuration parameters.

Echo Cancellation

- **Echo cancellation is configured at the voice port level.**
- **Echo cancellation is enabled by default.**
- **Echo cancellation coverage adjusts the size of the echo canceller.**
- **Nonlinear echo cancellation shuts off any signal if near-end speech is detected.**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2-7

Echo cancellation is configured at the voice port level. It is enabled by default and its characteristics are configurable. Echo cancellation commands are as follows:

- **echo-cancel enable:** This command enables cancellation of voice that is sent out through the interface and received back on the same interface. This sound is perceived by the listener as echo. Echo cancellation keeps a certain-sized sample of the outbound voice and calculates what that same signal looks like when it returns as an echo. Echo cancellation then attenuates the inbound signal by that amount to cancel the echo signal. If you disable echo cancellation, it will cause the remote side of a connection to hear echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, you should disable this command if it is not needed. There is no echo path for a four-wire E&M interface. The echo canceller should be disabled for this interface type.

Note This command is valid only if the **echo-cancel coverage** command has been configured.

- **echo-cancel coverage:** This command adjusts the coverage size of the echo canceller. This command enables cancellation of voice that is sent out through the interface and received back on the same interface within the configured amount of time. If the local loop (the distance from the interface to the equipment that is producing the echo) is longer, the configured value of this command should be extended.

If you configure a longer value for this command, it takes the echo canceller longer to converge. In this case, the user may hear a slight echo when the connection is initially set up. If the configured value for this command is too short, the user may hear some echo for the duration of the call, because the echo canceller is not canceling the longer-delay echoes.

There is no echo or echo cancellation on the network side of the connection that is not using plain old telephone service (POTS).

Note The **echo-cancel coverage** command is valid only if the echo cancel feature has been enabled.

- **non-linear:** The function enabled by the **non-linear** command is also known as residual echo suppression. This command effectively creates a half-duplex voice path. If voice is present on the inbound path, there is no signal on the outbound path. This command is associated with the echo canceller operation. The **echo-cancel enable** command must be enabled for the **non-linear** command to be available. Use the **non-linear** command to shut off any signal if near-end speech is not detected.

Enabling the **non-linear** command normally improves performance. However, some users encounter truncation of consonants at the ends of sentences when this command is enabled. This occurs when one person is speaking and the other person starts to speak before the first person finishes. Because the nonlinear cancellation allows speech in one direction only, it must switch directions on the fly. This may clip the end of the sentence spoken by the first person or the beginning of the sentence spoken by the second person.

Caution Do not use the echo cancellation commands or adjust voice quality unless you are experienced in doing so. Arbitrarily adjusting these parameters could adversely affect voice quality.

ITU standard G.164 defines the performance of echo suppressors, which are the predecessors of echo cancellation technology. G.164 also defines the disabling of echo suppressors in the presence of 2100 Hz tones that precede low-bit-rate modems.

ITU standard G.165 defines echo cancellation and provides a number of objective tests that ensure a minimum level of performance. These tests check convergence speed of the echo canceller, stability of the echo canceller filter, performance of the nonlinear processor, and a limited amount of double-talk testing. The signal used to perform these tests is white noise. Additionally, G.165 defines the disabling of echo cancellers in the presence of 2100 Hz signals with periodic phase reversals to support echo-canceling modem technology (for example, V.34). These do not work if line echo cancellation is performed in the connection.

ITU standard G.168 allows more rigorous testing and satisfies more testing requirements. White noise is replaced with a pseudo-speech signal for the convergence tests. Most echo cancellation algorithms use a least mean square algorithm to adapt the echo cancellation filter. This algorithm works best with random signals, and slows down with more correlated signals such as speech. Use of the pseudo-speech signal in testing provides a more realistic portrayal of the performance of the echo canceller in real use.

Example: Echo Suppression Applied

If you speak into your telephone and hear your own voice a short time later, you are experiencing talker echo. Talker echo is caused by the two-wire to four-wire hybrid circuit of the remote telephony circuitry. Enabling echo cancellation on your voice port will eliminate the problem. Depending on the return time of the echoed voice, you can make a further adjustment using the **echo-cancel coverage** command.

Echo Cancellor Comparison

This table contains echo canceller comparison information.

Echo Cancellor Comparison

	G.165 Echo Cancellor	G.168 Echo Cancellor
Tail Coverage	Up to 32 ms	Up to 64 ms
Minimum ERL	Greater than or equal to -6 dB	Configurable to greater than or equal to -0 dB, -3 dB, or -6 dB
Echo Suppression	Up to 10 seconds	Not required because of faster convergence
Minimum Cisco IOS Software Release	Cisco IOS Release 12.2(11)T, Cisco IOS Release 12.2(8)T5, Cisco IOS Release 12.2(12), and higher	Cisco IOS Release 12.2(13)T, Cisco IOS Release 12.2(8)YN, Cisco IOS Release 12.2(15)T, Cisco IOS Release 12.3(4)T, Cisco IOS Release 12.3(4)XD, and higher

Summary

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

Summary

- **Voice quality is affected by the settings on each voice port. Factors that affect voice quality include transmit and receive power levels, input gain, and output attenuation.**
- **Input and output power levels must be configured to match the connected devices.**
- **If the impedance is set incorrectly (if there is an impedance mismatch), a significant amount of echo is generated. Impedance settings must match the connecting equipment.**
- **To eliminate echo on a voice call, you can configure echo cancellation using the echo-cancel enable, echo-cancel coverage, and non-linear commands.**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2-8

References

For additional information, refer to this resource:

- *Configuring Voice Ports* (Voice Quality Tuning Commands).
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvfax_c/vvfpo-rt.htm#56672.

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 2-2: Configuring Voice Interfaces

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 factor can cause echo during transmission of voice over an IP network?
- A) The input level is too high.
 - B) The output level is too high at the remote router.
 - C) The local router voice port input is too low.
 - D) The input filter is configured improperly.
- Q2) At which receive level will analog voice routers operate best?
- A) -2 dB
 - B) -3 dB
 - C) -9 dB
 - D) -14 dB
- Q3) Which notation is used to indicate changes in signal strength?
- A) MHz
 - B) dB
 - C) PCM
 - D) ohms
- Q4) How does a user determine the appropriate signal strength required on a voice port?
- A) Signal strength is always dictated by the PSTN.
 - B) Signal strength must always be adjusted by -9 dB on all voice ports.
 - C) Signal strength should match the lowest PBX setting.
 - D) Signal strength must be configured to match the connected devices.
- Q5) Which two commands can be configured on an FXO voice port? (Choose two.)
- A) **input-gain**
 - B) **echo-cancel enable**
 - C) **impedance**
 - D) **echo-cancel coverage**
 - E) **output-attenuation**
- Q6) When is the best time to change default voice port configurations?
- A) before you set up the network
 - B) after the network is up and running
 - C) after two dial peers experience poor quality
 - D) when there is a network failure
- Q7) Which command is used to enable residual echo suppression?
- A) **echo-cancel enable**
 - B) **echo-cancel coverage**
 - C) **non-linear**
 - D) **no echo-cancel enable**

- Q8) Which of these commands is enabled by default?
- A) **echo-cancel enable**
 - B) **echo-cancel coverage**
 - C) **non-linear**
 - D) **no echo-cancel enable**
- Q9) If the echo coverage interval is set too long, what is the impact?
- A) There may be residual echo.
 - B) The user may hear a slight echo when the connection is initially set up.
 - C) The user may hear some echo for the duration of the call.
 - D) The user may experience clipping at the end of sentences.

Lesson Self-Check Answer Key

- Q1) B
Relates to: Factors Affecting Voice Quality
- Q2) B
Relates to: Factors Affecting Voice Quality
- Q3) B
Relates to: Setting Input and Output Power Levels
- Q4) D
Relates to: Setting Input and Output Power Levels
- Q5) D, E
Relates to: Voice Quality Tuning
- Q6) B
Relates to: Voice Quality Tuning
- Q7) C
Relates to: Echo Cancellation Commands
- Q8) A
Relates to: Echo Cancellation Commands
- Q9) A
Relates to: Echo Cancellation Commands

Lesson 3

Configuring Dial Peers

Overview

This lesson describes call flows as they relate to inbound and outbound dial peers, voice dial peers, hunt groups, digit manipulation, and the matching of calls to dial peers.

Relevance

As a call is set up across the network, the existence of various parameters is checked and negotiated. A mismatch in parameters can cause call failure. It is important to understand how routers interpret call legs and how call legs relate to inbound and outbound dial peers. Successful implementation of a Voice over IP (VoIP) network relies heavily on the proper application of dial peers, the digits they match, and the services they specify. The network engineer must have in-depth knowledge of dial-peer configuration options and their uses. This lesson discusses the proper use of digit manipulation and the configuration of dial peers.

Objectives

Upon completing this lesson, you will be able to describe how call legs relate to inbound and outbound dial peers by following all the steps in the call setup process. You will also be able to describe the proper use of digit manipulation and configuration of dial peers to implement a successful VoIP network. This ability includes being able to meet these objectives:

- Describe call legs and their relationships to other components
- Describe how call legs are interpreted by routers to establish end-to-end calls
- Describe dial peers and their application
- Configure POTS dial peers
- Configure VoIP dial peers
- Describe destination-pattern options and the applicable shortcuts
- Describe the default dial peer
- Describe how the router matches inbound dial peers
- Describe how the router matches outbound dial peers
- Configure hunt groups

- Describe how the router and the attached telephony equipment collect and consume digits, and apply the digits to the dial peer
- Describe digit manipulation and the commands that are used to connect to a specified destination

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Familiarity with Cisco IOS configuration modes
- Familiarity with call-routing concepts and voice ports
- Familiarity with telephony concepts

Outline

The outline lists the topics included in this lesson.

Outline

- **Overview**
- **Dial Peers and Call Legs**
- **End-to-End Calls**
- **Types of Dial Peers**
- **Configuring POTS Dial Peers**
- **Configuring VoIP Dial Peers**
- **Configuring Destination-Pattern Options**
- **Default Dial Peer**
- **Matching Inbound Dial Peers**
- **Matching Outbound Dial Peers**
- **Configuring Hunt Groups**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0—2-2

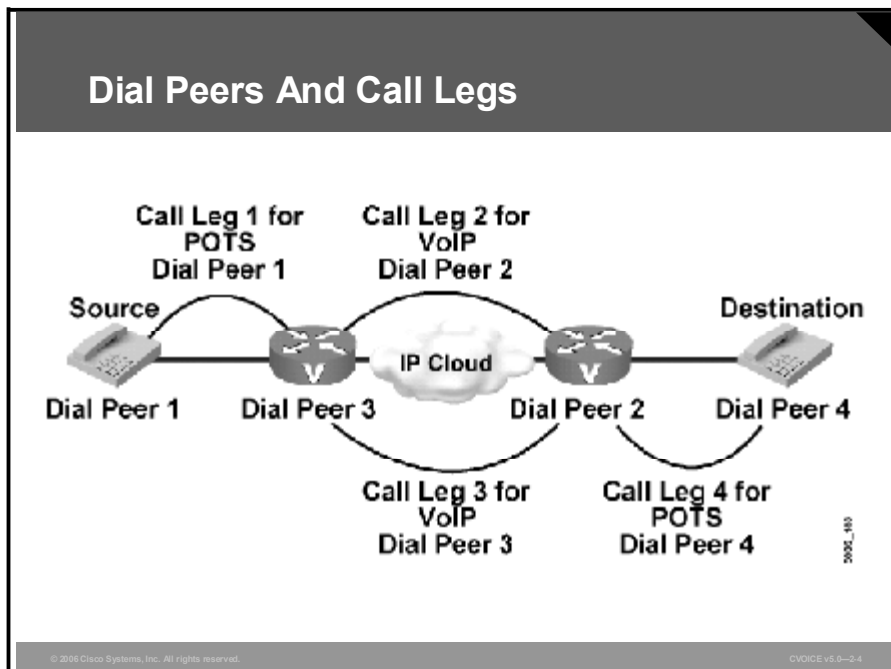
Outline (Cont.)

- **Digit Collection and Consumption**
- **Configuring Digit Manipulation**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0—2-3

Dial Peers and Call Legs

This topic describes call legs and their relationship to other components.



Call legs are logical connections between any two telephony devices, such as gateways, routers, Cisco CallManagers, or telephony endpoint devices.

Call legs are router-centric. When an inbound call arrives, it is processed separately until the destination is determined. Then a second outbound call leg is established, and the inbound call leg is switched to the outbound voice port.

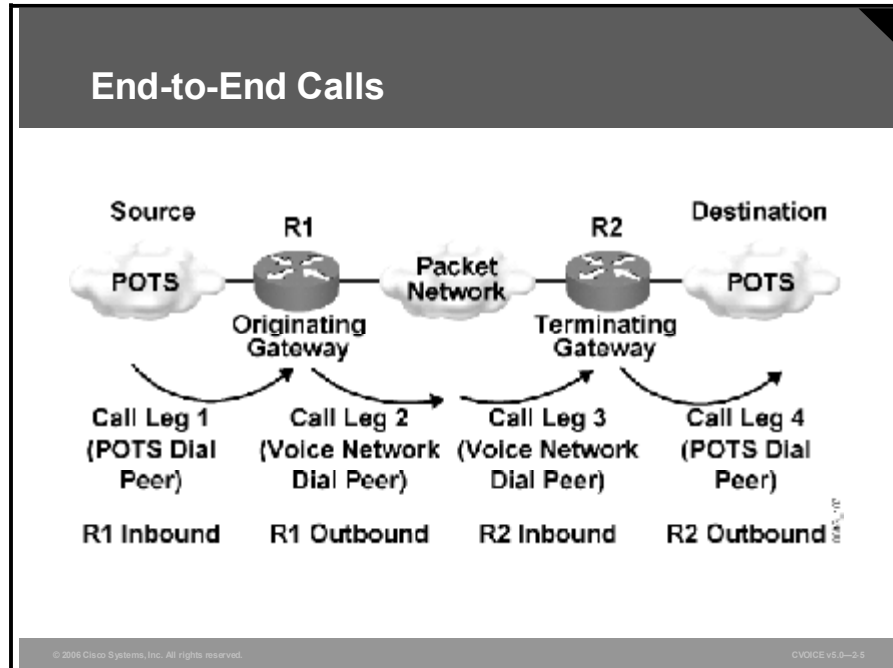
Example: Call Legs Defined

The connections are made when you configure dial peers on each interface. An end-to-end call consists of four call legs: two from the source router perspective (as shown in the figure), and two from the destination router perspective. To complete an end-to-end call from either side and send voice packets back and forth, you must configure all four dial peers.

Dial peers are used only to set up calls. After the call is established, dial peers are no longer employed.

End-to-End Calls

This topic explains how routers interpret call legs to establish end-to-end calls.



An end-to-end voice call consists of four call legs: two from the originating router (R1) or gateway perspective, and two from the terminating router (R2) (refer to the figure) or gateway perspective. An inbound call leg occurs when an incoming call comes *into* the router or gateway. An outbound call leg occurs when a call is placed *from* the router or gateway.

A call is segmented into call legs, and a dial peer is associated with each call leg. The process for call setup is listed here:

1. The plain old telephone service (POTS) call arrives at R1 and an inbound POTS dial peer is matched.
2. After associating the incoming call to an inbound POTS dial peer, R1 creates an inbound POTS call leg and assigns it a Call ID (call leg 1).
3. R1 uses the dialed string to match an outbound voice network dial peer.
4. After associating the dialed string to an outbound voice network dial peer, R1 creates an outbound voice network call leg and assigns it a Call ID (call leg 2).
5. The voice network call request arrives at R2 and an inbound voice network dial peer is matched.
6. After R2 associates the incoming call to an inbound voice network dial peer, R2 creates the inbound voice network call leg and assigns it a Call ID (call leg 3). At this point, both R1 and R2 negotiate voice network capabilities and applications, if required.

The originating router or gateway may request nondefault capabilities or applications. When this is the case, the terminating router or gateway must match an inbound voice network dial peer that is configured for such capabilities or applications.

7. R2 uses the dialed string to match an outbound POTS dial peer.
8. After associating the incoming call setup with an outbound POTS dial peer, R2 creates an outbound POTS call leg, assigns it a Call ID, and completes the call (call leg 4).

Types of Dial Peers

This topic describes dial peers and their applications.

Types of Dial Peers

- **A dial peer is an addressable call endpoint.**
- **Dial peers establish logical connections, called call legs, to complete an end-to-end call.**
- **Cisco voice-enabled routers support two types of dial peers:**
 - **POTS dial peers: Connect to a traditional telephony network**
 - **VoIP dial peers: Connect over a packet network**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2.6

When a call is placed, an edge device generates dialed digits as a way of signaling where the call should terminate. When these digits enter a router voice port, the router must decide whether the call can be routed, and where the call can be sent. The router does this by searching a list of dial peers.

A dial peer is an addressable call endpoint. The address is called a destination pattern and is configured in every dial peer. Destination patterns can point to one telephone number or to a range of telephone numbers. Destination patterns use both explicit digits and wildcard variables to define a telephone number or range of numbers.

The router uses dial peers to establish logical connections. These logical connections, known as call legs, are established in either an inbound or outbound direction.

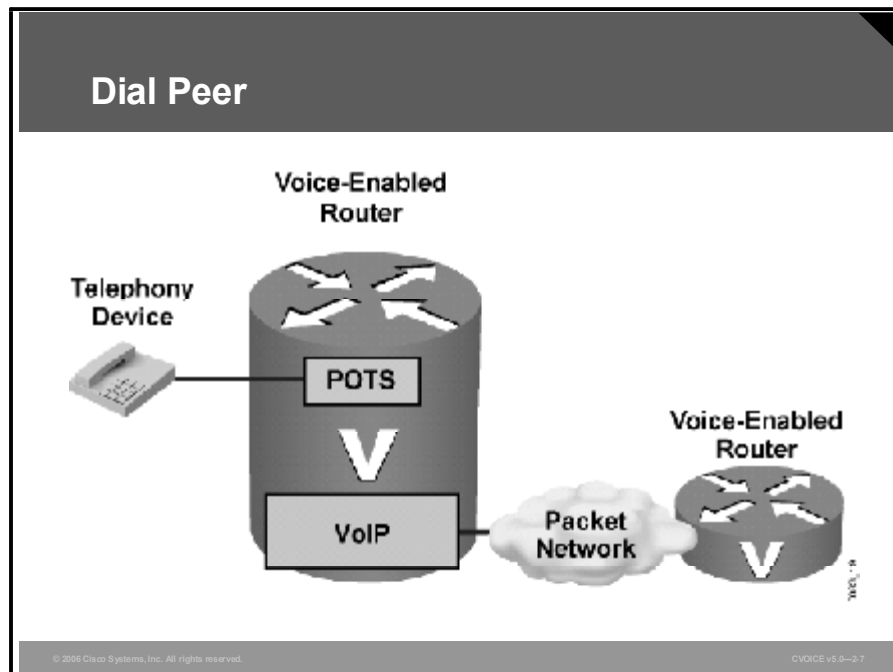
Dial peers define the parameters for the calls that they match. For example, if a call is originating and terminating at the same site, and is not crossing through slow-speed WAN links, the call can cross the local network uncompressed and without special priority. A call that originates locally and crosses the WAN link to a remote site may require compression with a specific coder-decoder (codec). In addition, this call may require that voice activity detection (VAD) be turned on, and will need to receive preferential treatment by specifying a higher priority level.

Cisco voice-enabled routers support two types of dial peers:

- **POTS dial peers:** **POTS dial peers** connect to a traditional telephony network, such as the public switched telephone network (PSTN) or a PBX, or to a telephony edge device such as a telephone or fax machine. POTS dial peers perform these functions:
 - Provide an address (telephone number or range of numbers) for the edge network or device
 - Point to the specific voice port that connects the edge network or device
- **VoIP dial peers:** **VoIP dial peers** connect over an IP network. VoIP dial peers perform these functions:
 - Provide a destination address (telephone number or range of numbers) for the edge device that is located across the network
 - Associate the destination address with the next-hop router or destination router, depending on the technology used

Example: Dial-Peer Configuration

This figure shows a dial-peer configuration.



In the figure, the telephony device connects to the Cisco voice-enabled router. The POTS dial-peer configuration includes the telephone number of the telephony device and the voice port to which it is attached. The router determines where to forward incoming calls for that telephone number.

The Cisco voice-enabled router VoIP dial peer is connected to the packet network. The VoIP dial-peer configuration includes the destination telephone number (or range of numbers) and the next-hop or destination voice-enabled router network address.

Follow the steps in the table to place a VoIP call.

How to Place a VoIP Call

Step	Action
1.	Configure a compatible dial peer on the source router that specifies the recipient destination address.
2.	Configure a POTS dial peer on the recipient router that specifies which voice port the router uses to forward the voice call.

Configuring POTS Dial Peers

This topic describes how to configure POTS dial peers.

POTS Dial Peers

Configuration for Dial Peer 1 on Router 1:

```

Router# configure terminal
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer)# destination-pattern 7777
Router(config-dialpeer)# port 1/0/0
Router(config-dialpeer)# end
    
```

© 2006 Cisco Systems, Inc. All rights reserved.
CVOICE v5.0-2.5

Before the configuration of Cisco IOS dial peers can begin, the user must have a good understanding of where the edge devices reside, what type of connections need to be made between these devices, and what telephone numbering scheme is applied to the devices.

Follow the steps in the table to configure POTS dial peers.

How to Configure POTS Dial Peers

Step	Action
1.	Configure a POTS dial peer at each router or gateway where edge telephony devices connect to the network.
2.	Use the destination-pattern command in the dial peer to configure the telephone number.
3.	Use the port command to specify the physical voice port that the POTS telephone is connected to.

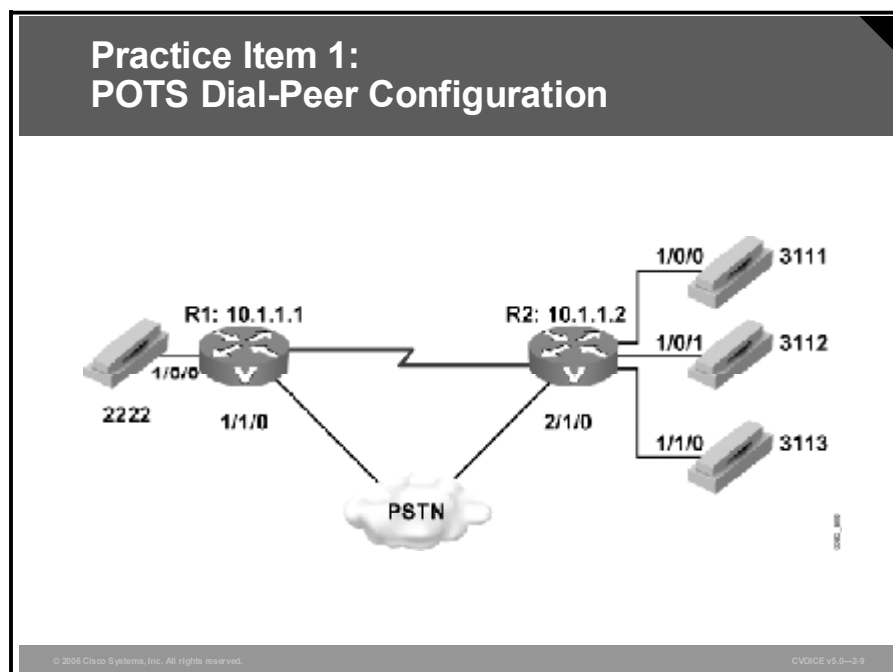
The dial-peer type will be specified as POTS because the edge device is directly connected to a voice port and the signaling must be sent from this port to reach the device. There are two basic parameters that need to be specified for the device: the telephone number and the voice port. When a PBX is connecting to the voice port, a range of telephone numbers can be specified.

Example: POTS Dial-Peer Configuration

The figure illustrates proper POTS dial-peer configuration on a Cisco voice-enabled router. The **dial-peer voice 1 pots** command notifies the router that dial peer 1 is a POTS dial peer with a tag of 1. The **destination-pattern 7777** command notifies the router that the attached telephony device terminates calls destined for telephone number 7777. The **port 1/0/0** command notifies the router that the telephony device is plugged into module 1, voice interface card (VIC) slot 0, and voice port 0.

Practice Item 1: POTS Dial-Peer Configuration

Throughout this lesson, you will practice what you have learned. In this scenario, assume that there is a data center at the R1 site, and executive offices at the R2 site. Using the diagram, create POTS dial peers for the four telephones shown.

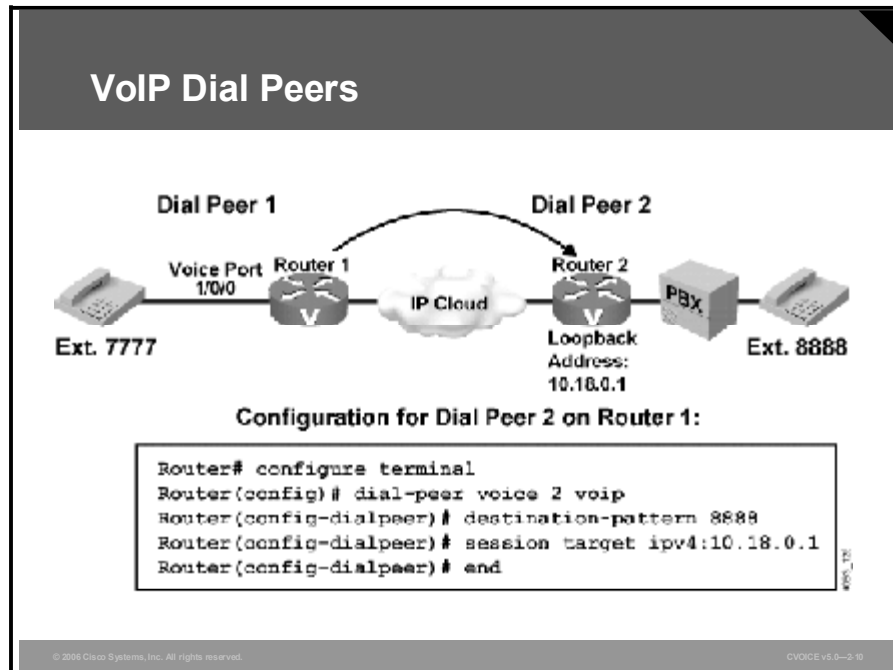


R1

R2

Configuring VoIP Dial Peers

This topic describes how to configure VoIP dial peers.



The administrator must know how to identify the far-end voice-enabled device that will terminate the call. In a small network environment, the device may be the IP address of the remote device. In a large environment, identifying the device may mean pointing to a Cisco CallManager or gatekeeper for address resolution and Call Admission Control (CAC) to complete the call.

You must follow the steps in the table to configure VoIP dial peers.

How to Configure VoIP Dial Peers

Step	Action
1.	Configure the path across the network for voice data.
2.	Specify the dial peer as a VoIP dial peer.
3.	Use the destination-pattern command to configure a range of numbers reachable by the remote router or gateway.
4.	Use the session target command to specify an IP address of the terminating router or gateway.
5.	Use the remote device loopback address as the IP address.

The dial peer is specified as a VoIP dial peer, which alerts the router that it must process a call according to the various dial-peer parameters. The dial peer must then package it as an IP packet for transport across the network. Specified parameters may include the codec used for compression (VAD, for example), or marking the packet for priority service.

The **destination-pattern** command configured for this dial peer is typically a range of numbers that are reachable via the remote router or gateway.

Because this dial peer points to a device across the network, the router needs a destination IP address to put in the IP packet. The **session target** command allows the administrator to specify either an IP address of the terminating router or gateway, or another device. For example, a gatekeeper or Cisco CallManager may return an IP address of that remote terminating device.

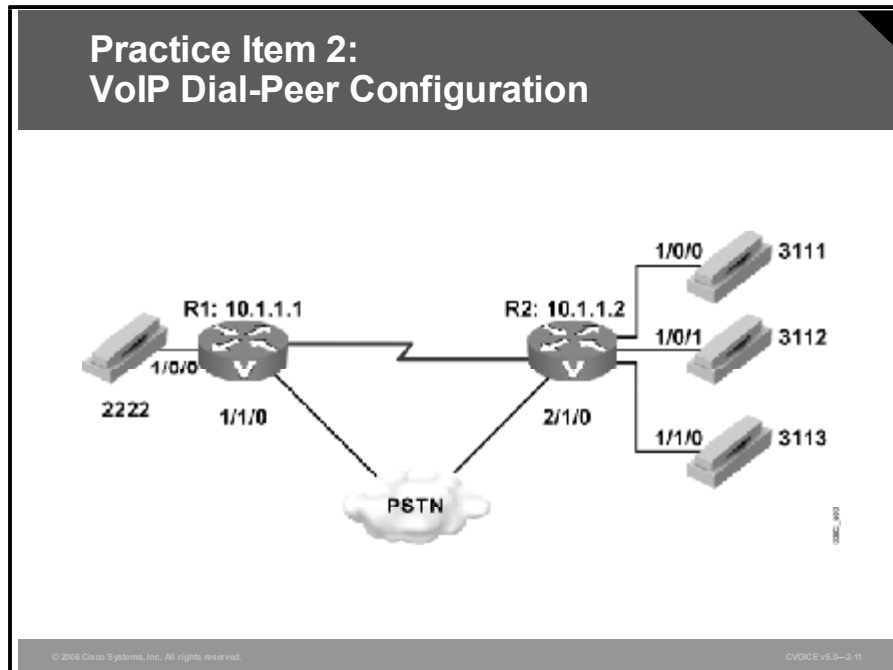
To determine which IP address a dial peer should point to, it is recommended that you use a loopback address. The loopback address is always up on a router, as long as the router is powered on and the interface is not administratively shut down. The reason an interface IP address is not recommended is that if the interface goes down, the call will fail even if there is an alternate path to the router.

Example: VoIP Dial-Peer Configuration

The figure illustrates the proper VoIP dial-peer configuration on a Cisco voice-enabled router. The **dial-peer voice 2 voip** command notifies the router that dial peer 2 is a VoIP dial peer with a tag of 2. The **destination-pattern 8888** command notifies the router that this dial peer defines an IP voice path across the network for telephone number 8888. The **session target ipv4:10.18.0.1** command defines the IP address of the router that is connected to the remote telephony device.

Practice Item 2: VoIP Dial-Peer Configuration

Create VoIP dial peers for each of the R1 and R2 sites according to this diagram.



R1

R2

Configuring Destination-Pattern Options

This topic describes destination-pattern options and the applicable shortcuts.

Common Destination-Pattern Options

Command Syntax: destination-pattern [+]*string* [T]

+	(Optional) Character indicating an E.164 standard number
<i>string</i>	<p>Series of digits that specify the E.164 or private dial plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and these special characters:</p> <ul style="list-style-type: none">• The asterisk (*) and pound sign (#) appear on standard touch-tone dial pads.• A comma (,) inserts a pause between digits.• A period (.) matches any single entered digit (this character is used as a wildcard).• Brackets ([]), indicate a range. A range is a sequence of characters enclosed in the brackets; only numeric characters from 0 to 9 are allowed in the range.
T	(Optional) Control character indicating that the destination-pattern value is a variable-length dial string

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2/12

The destination pattern associates a telephone number with a given dial peer. It also determines the dialed digits that the router collects and forwards to the remote telephony interface, such as a PBX, Cisco CallManager, or the PSTN. You must configure a destination pattern for each POTS and VoIP dial peer that you define on the router.

The destination pattern can indicate a complete telephone number, a partial telephone number with wildcard digits, or it can point to a range of numbers defined in a variety of ways.

Destination-pattern options include those listed here:

- **Plus sign (+):** This is an optional character that indicates an E.164 standard number. E.164 is the ITU-T recommendation for the international public telecommunication numbering plan. The plus sign in front of a destination-pattern string specifies that the string must conform to E.164.
- **string:** This is a series of digits specifying the E.164 or private dial plan telephone number. The examples that follow show the use of special characters that are often found in destination pattern strings:
 - An asterisk (*) and pound sign (#) appear on standard touch-tone dial pads. These characters may need to be used when passing a call to an automated application that requires these characters to signal the use of a special feature. For example, when calling an interactive voice response (IVR) system that requires a code for access, the number dialed might be “5551212888#”, which would initially dial the telephone number “5551212” and input a code of “888” followed by the pound key to terminate the IVR input query.

- A comma (,) inserts a 1-second pause between digits. The comma can be used, for example, where a “9” is dialed to signal a PBX that the call should be processed by the PSTN. The “9” is followed by a comma to give the PBX time to open a call path to the PSTN, after which the remaining digits will be played out. An example of this string is “9,5551212”.
 - A period (.) matches any single entered digit from 0 to 9, and is used as a wildcard. The wildcard can be used to specify a group of numbers that may be accessible via a single destination router, gateway, PBX, or Cisco CallManager. A pattern of “200.” allows for 10 uniquely addressed devices, while a pattern of “20.” can point to 100 devices. If one site has the numbers 2000 through 2049, and another site has the numbers 2050 through 2099, the bracket notation would be more efficient.
 - Brackets ([]) indicate a range. A range is a sequence of characters that are enclosed in the brackets. Only single numeric characters from 0 to 9 are allowed in the range. In the previous example, the bracket notation could be used to specify exactly which range of numbers is accessible through each dial peer. For example, the first site pattern would be “20[0 – 4].”, and the second site pattern would be “20[5-9].”. Note that in both cases, a dot is used in the last digit position to represent any single digit from 0 to 9. The bracket notation offers much more flexibility in how numbers can be assigned.
- **T:** This is an optional control character indicating that the destination-pattern value is a variable-length dial string. In cases where callers may be dialing local, national, or international numbers, the destination pattern must provide for a variable-length dial plan. If a particular voice gateway has access to the PSTN for local calls and access to a transatlantic connection for international calls, calls being routed to that gateway will have a varying number of dialed digits. A single dial peer with a destination pattern of “.T” could support the different call types. The **interdigit timeout** command determines when a string of dialed digits is complete. The router continues to collect digits until there is an interdigit pause longer than the configured value, which by default is 10 seconds.

When the calling party finishes entering dialed digits, there is a pause equal to the interdigit timeout value *before* the router processes the call. The calling party can immediately terminate the interdigit timeout by entering the pound character (#), which is the default termination character. Because the default interdigit timer is set to 10 seconds, users may experience a long call setup delay.

Note Cisco IOS software does not check the validity of the E.164 telephone number. It accepts any series of digits as a valid number.

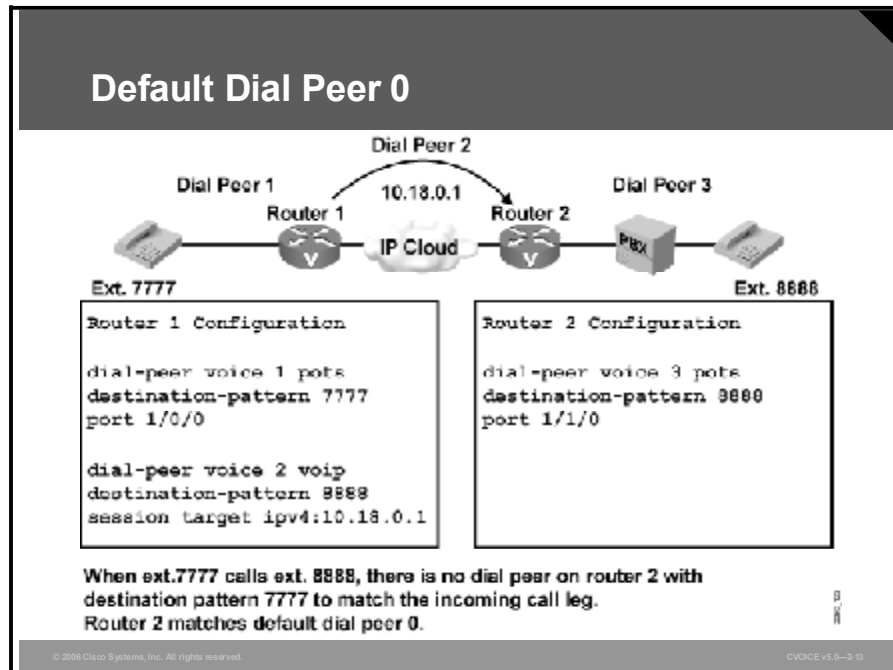
Example: Matching Destination Patterns

Destination-Pattern Options

Destination Pattern	Matching Telephone Numbers
5550124	<p>This destination pattern matches one telephone number exactly, 5550124.</p> <p>This is typically used when there is a single device, such as a telephone or fax, connected to a voice port.</p>
55501[1-3].	<p>This destination pattern matches a seven-digit telephone number where the first five digits are 55501, the sixth digit can be a 1, 2, or 3, and the last digit can be any valid digit.</p> <p>This type of destination pattern is used when telephone number ranges are assigned to specific sites. In this example, the destination pattern is used in a small site that does not need more than 30 numbers assigned.</p>
.T	<p>This destination pattern matches any telephone number that has at least 1 digit and can vary in length from 1 to 32 digits total.</p> <p>This destination pattern is used for a dial peer that services a variable-length dial plan, for local, national, and international calls. It can also be used as a default destination pattern so that any calls that do not match a more specific pattern will match this pattern and can be directed to an operator.</p>

Default Dial Peer

This topic describes the default dial peer.



When a matching inbound dial peer is not found, the router resorts to the default dial peer.

Note Default dial peers are used for inbound matches only. They are not used to match outbound calls that do not have a dial peer configured.

The default dial peer is referred to as dial peer 0.

Example: Use of Default Dial Peer

In the figure, only one-way dialing is configured. The caller at extension 7777 can call extension 8888 because there is a VoIP dial peer configured on router 1 to route the call across the network. There is no VoIP dial peer configured on router 2 to point calls across the network toward router 1. Therefore, there is no dial peer on router 2 that will match the calling number of extension 7777 on the inbound call leg. If no incoming dial peer matches the calling number, the inbound call leg automatically matches to a default dial peer (POTS or VoIP).

Note Cisco voice and dial platforms, such as the AS5300 Series Universal Gateways and Cisco AS5800 Series Universal Gateways, require that a configured inbound dial peer be matched for incoming POTS calls to be accepted as voice calls. If there is no inbound dial-peer match, the call is treated and processed as a dialup (modem) call.

Dial peer 0 for inbound VoIP peers has this configuration:

- **any codec**
- **ip precedence 0**
- **vad enabled**
- **no rsvp support**
- **fax-rate service**

Dial peer 0 for inbound POTS peers has this configuration:

- **no ivr application**

You cannot change the default configuration for dial peer 0. Default dial peer 0 fails to negotiate nondefault capabilities or services. When the default dial peer is matched on a VoIP call, the call leg that is set up in the inbound direction uses any supported codec for voice compression that is based on the requested codec capability coming from the source router. When a default dial peer is matched, the voice path in one direction may have different parameters than the voice in the return direction. This may cause one side of the connection to report good quality voice while the other side reports poor quality voice. For example, the outbound dial peer has VAD disabled, but the inbound call leg is matched against the default dial peer, which has VAD enabled. VAD would be on in one direction and off in the return direction.

When the default dial peer is matched on an inbound POTS call leg, there is no default IVR application with the port. As a result, the user gets a dial tone and proceeds with dialed digits.

Matching Inbound Dial Peers

This topic describes how the router matches with inbound dial peers.

Matching Inbound Dial Peers

Configurable parameters used for matching inbound dial peers:

- incoming called-number
 - **Defines the called number or DNIS string**
- answer-address
 - **Defines the originating calling number or ANI string**
- destination-pattern
 - **Uses the calling number (originating or ANI string) to match the incoming call leg to an inbound dial peer**
- port
 - **Attempts to match the configured dial-peer port to the voice port associated with the incoming call (POTS dial peers only)**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v9.0-2-14

When determining how inbound dial peers are matched on a router, it is important to note whether the inbound call leg is matched to a POTS or VoIP dial peer. Matching occurs in the following manner:

- Inbound POTS dial peers are associated with the incoming POTS call legs of the originating router or gateway.
- Inbound VoIP dial peers are associated with the incoming VoIP call legs of the terminating router or gateway.

Three information elements sent in the call setup message are matched against four configurable dial-peer command attributes.

The table describes the three call setup information elements.

Call Setup Information Elements

Call Setup Element	Description
Called number Dialed Number Identification Service (DNIS)	This is the call destination dial string, and it is derived from the ISDN setup message or channel associated signaling the DNIS.
Calling number automatic number identification (ANI)	This is a number string that represents the origin, and it is derived from the ISDN setup message or channel associated signaling (CAS) ANI. The ANI is also referred to as the calling line ID (CLID).
Voice port	This represents the POTS physical voice port.

When the Cisco IOS router or gateway receives a call setup request, it looks for a dial-peer match for the incoming call. This is not digit-by-digit matching. Instead, the router uses the full digit string received in the setup request for matching against the configured dial peers.

The router or gateway matches call setup element parameters in the order listed in the table.

How the Router or Gateway Matches Inbound Dial Peers

Step	Action
1.	The router or gateway attempts to match the called number of the call setup request with the configured incoming called-number parameter of each dial peer.
2.	If a match is not found, the router or gateway attempts to match the calling number of the call setup request with the answer-address parameter of each dial peer.
3.	If a match is not found, the router or gateway attempts to match the calling number of the call setup request to the destination-pattern parameter of each dial peer.
4.	The voice port uses the voice port number associated with the incoming call setup request to match the inbound call leg to the configured dial peer port parameter.
5.	If multiple dial peers have the same port configured, the router or gateway matches the first dial peer added to the configuration.
6.	If a match is not found in the previous steps, the default is dial peer 0.

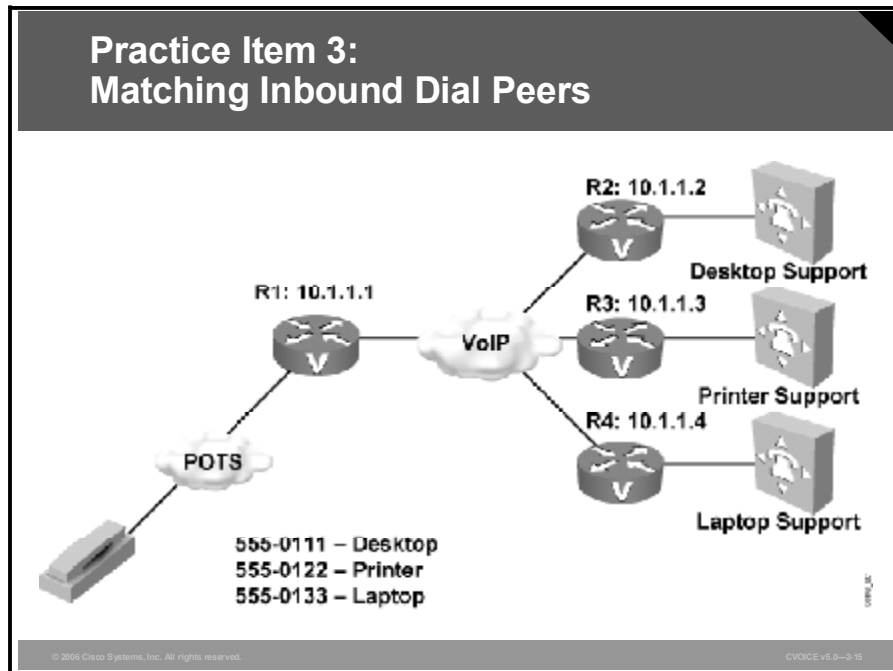
Because call setups always include DNIS information, it is recommended that you use the **incoming called-number** command for inbound dial-peer matching. Configuring **incoming called-number** command is useful for a company that has a central call center providing support for a number of different products. Purchasers of each product get a unique toll-free number to call for support. All support calls are routed to the same trunk group destined for the call center. When a call comes in, the computer telephony system uses the DNIS to flash the appropriate message on the computer screen of the agent to whom the call is routed. The agent will then know how to customize the greeting when answering the call.

The calling number ANI with **answer-address** command is useful when you want to match calls based on the originating calling number. For example, when a company has international customers who require foreign-language-speaking agents to answer the call, the call can be routed to the appropriate agent based on the country of call origin.

You must use the calling number ANI with the **destination-pattern** command when the dial peers are set up for two-way calling. In a corporate environment, the head office and the remote sites must be connected. As long as each site has a VoIP dial peer configured to point to each site, inbound calls from the remote site will match against that dial peer.

Practice Item 3: Matching Inbound Dial Peers

In this practice item, assume that you are setting up a technical support center for desktop PCs, printers, and laptops. Customers who dial specific numbers need to reach the appropriate technical support staff. Using the diagram, create dial peers on R1 to route incoming calls by the incoming called number to the appropriate site.



R1

Matching Outbound Dial Peers

This topic describes how the router matches outbound dial peers.

Matching Outbound Dial Peers

The destination pattern is matched based on the longest number match.

```
dial-peer voice 1 voip
destination-pattern .1
session target ipv4 10.1.1.1

dial-peer voice 2 voip
destination-pattern 5501[3-6].
session target ipv4 10.2.2.2

dial-peer voice 3 voip
destination-pattern 55012.
session target ipv4 10.3.3.3

dial-peer voice 4 voip
destination-pattern 550124
session target ipv4 10.4.4.4
```

Example 1: Dialed number 555-0124 will match dial peer 4.
Example 2: Dialed number 555-0126 will match dial peer 3.
Example 3: Dialed number 555-0135 will match dial peer 2.
Example 4: Dialed number 555-0199 will match dial peer 1.

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-2/16

Outbound dial-peer matching is completed on a digit-by-digit basis. Therefore, the router or gateway checks for dial-peer matches after receiving each digit and then routes the call when a full match is made.

The router or gateway matches outbound dial peers in the order listed in the table.

How the Router or Gateway Matches Outbound Dial Peers

Step	Action
1.	The router or gateway uses the dial peer destination-pattern command to determine how to route the call.
2.	The destination-pattern command routes the call in the following manner: <ul style="list-style-type: none">■ On POTS dial peers, the port command forwards the call.■ On VoIP dial peers, the session target command forwards the call.
3.	Use the show dialplan number string command to determine which dial peer is matched to a specific dialed string. This command displays all matching dial peers in the order that they are used.

Example: Matching Outbound Dial Peers

In the figure, dial peer 1 matches any digit string that does not match the other dial peers more specifically. Dial peer 2 matches any 7-digit number in the 30 and 40 range of numbers starting with 55501. Dial peer 3 matches any 7-digit number in the 20 range of numbers starting with 55501. Dial peer 4 matches the specific number 5550124 only. When the number 5550124 is dialed, dial peers 1, 3, and 4 all match that number, but dial peer 4 places that call because it contains the most specific destination pattern.

Configuring Hunt Groups

This topic describes hunt group commands and how to configure hunt groups.

Hunt-Group Commands

- Preference (**dial-peer command**)
 - Specifies which dial peers in a hunt group will be used first
 - Options are 0 through 9, with 0 being most preferred
- Huntstop (**dial-peer command**)
 - Stops dial-peer hunting on the dial peer if it is not matched
- dial-peer hunt (**global command**)
 - Specifies the global hunt-selection order for all hunt groups

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2/17

Cisco voice-enabled routers support the concept of hunt groups, sometimes called rotary groups, in which multiple dial peers are configured with the same destination pattern. The destination of each POTS dial peer is a single voice port to a telephony interface, so hunt groups help ensure that calls get through even when a specific voice port is busy. If the router is configured to hunt, it can forward a call to another voice port that is not busy.

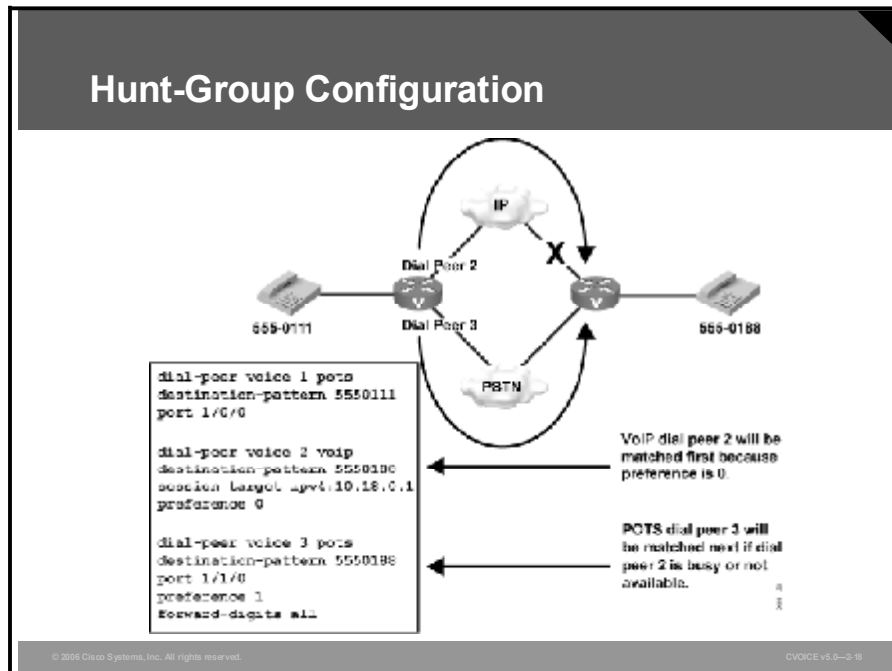
Here is a list of hunt-group commands:

- **preference:** This command sets priority for dial peers. The destination with the lowest setting has the highest priority.
- **huntstop:** This command disables dial-peer hunting on the dial peer.
- **dial-peer hunt:** This command changes the default selection order for hunting through dial peers.

You can also use this command to view dial-peer hunt current settings:

- **show dial-peer voice summary:** This command shows the current settings for dial-peer hunt.

Hunt-Group Configuration



In some business environments, such as call centers or sales departments, there may be a group of agents available to answer calls coming in to a single number. Scenario 1 may randomly distribute the calls between all agents. Scenario 2 may send calls to the senior agents first, and send calls to the junior agents only when all senior agents are busy. Both of these scenarios can be serviced by configuring a hunt group with specific commands to control the hunt actions.

Follow the steps in the table to configure hunt groups.

How to Configure Hunt Groups

Step	Action
1.	Configure the same destination pattern across multiple dial peers.
2.	The destination pattern matches the greatest number of dialed digits.
3.	Use the preference command if the destination pattern of the dial peer is the same for several dial peers.
4.	If the preference does not act as the tiebreaker, the router picks the matching dial peer randomly.

You must use the **dial-peer hunt** global configuration command to change the default selection order of the procedure or to choose different methods for hunting through dial peers. To view the current setting for **dial-peer hunt** command, use the **show dial-peer voice summary** command.

If you do not want to hunt through a range of dial peers, the **huntstop** command disables dial-peer hunting. After you enter this command, no further hunting is allowed if a call fails on the selected dial peer. This is useful in situations where it is undesirable to hunt to a less specific dial peer if the more specific call fails. For example, if a call is destined for a particular staff member and the person is on the phone, the router searches for any other dial peer that may match the dialed number. If there is a more generic destination pattern in another dial peer that also matches, the call is routed to the generic destination pattern. Configuring the **huntstop** command in the more specific dial peer will send the caller a busy signal.

You can mix POTS and VoIP dial peers when creating hunt groups. This is useful if you want incoming calls sent over the packet network but network connectivity fails. You can then reroute the calls back through the PBX, or through the router, to the PSTN.

By default, the router selects dial peers in a hunt group according to the criteria in the table, in the order listed.

How the Router Selects Dial Peers in a Hunt Group

Step	Action
1.	The router matches the most specific telephone number.
2.	The router matches according to the preference setting.
3.	The router matches randomly.

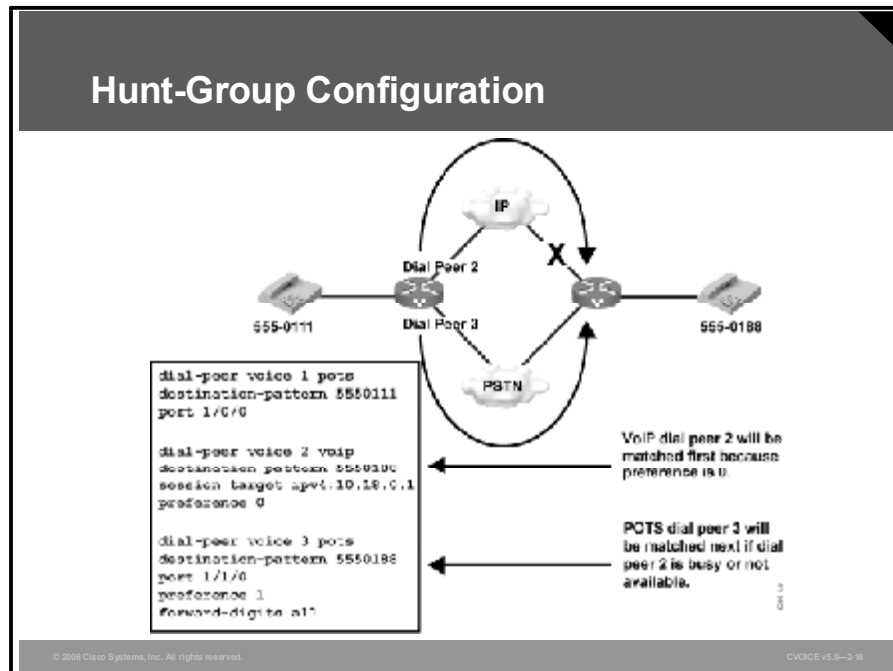
The destination pattern that matches the greatest number of dialed digits is the first dial peer selected by the router. For example, if one dial peer is configured with a dial string of “345....” and a second dial peer is configured with “3456789”, the router selects “3456789” first because it has the longest explicit match of the two dial peers. Without a PBX, if the line is currently in use, the desired action is to send a call to a voice-mail system or to an administrative employee, instead of giving the caller a busy signal.

If the destination pattern is the same for several dial peers, you can configure the priority by using the **preference** dial-peer command. This would be the configuration for scenario 2, where the dial peers connecting to the senior agents would have **preference 0** and the dial peers connecting to the junior agents would have **preference 1**. The lower the preference is set, the more likely that dial peer will handle the call.

By default, if all destination patterns are equal, the preference is set to 0 on all dial peers. If the preference does not act as the tiebreaker, a dial peer matching the called number will be picked randomly. This would be the configuration for scenario 1.

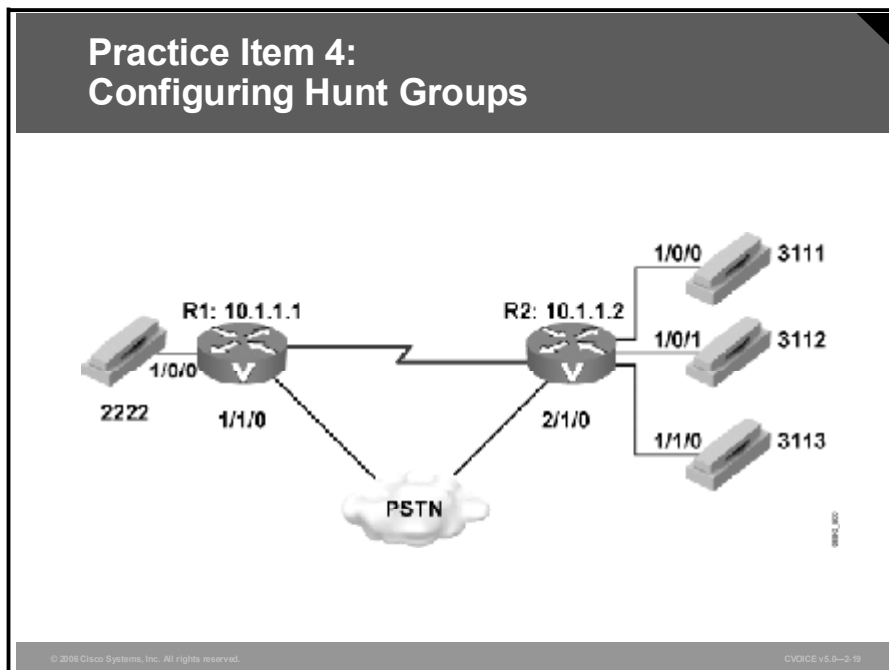
Example: Hunt-Group Application

The figure shows an example of configuring a hunt group to send calls to the PSTN if the IP network fails. For all calls going to 555-0188, VoIP dial peer 2 is matched first because the preference is set to 0. If the path through the IP network fails, POTS dial peer 3 is matched and the call is forwarded through the PSTN. The **forward-digits** command forwards all digits to the PSTN to automatically complete the call without a secondary dial tone.



Practice Item 4: Configuring Hunt Groups

Consider this diagram. Create a hunt group using the **preference** command on R2. Configure the hunt group so that if extension 3111 is busy, the call rings extension 3112. Assume that you have POTS dial peers for all three extensions already configured.



R2: Already configured

```
dial-peer voice 1 pots
destination-pattern 3111
port 1/0/0
```

```
dial-peer voice 2 pots
destination-pattern 3112
port 1/0/1
```

```
dial-peer voice 3 pots
destination-pattern 3113
port 1/1/0
```

R2: Hunt group dial peer

Digit Collection and Consumption

This topic describes how the router collects and consumes digits and applies them to the dial-peer statements.

Digit Consumption and Forwarding

- **POTS dial peers:**
 - By default, the router consumes the left-justified digits that explicitly match the destination pattern and forwards wildcarded digits.
 - Use the `no digit-strip` command to disable the automatic digit-stripping function.
- **VoIP dial peers:** By default, the router forwards all digits collected.

Example 1: Dialed digits 5550124

```
dial-peer voice 1 pots
destination-pattern 555....
port 1/0:1
```

Explicitly matched digits 555 are consumed and 0124 is forwarded.

Example 2: Dialed digits 5550124

```
dial-peer voice 1 pots
destination-pattern 555....
no digit-strip
port 1/0:1
```

Digits 5550124 are forwarded.

© 2006 Cisco Systems, Inc. All rights reserved. VOICE vs.0-2.0

Use the **no digit-strip** command to disable the automatic digit-stripping function. This allows the router to match digits and pass them to the telephony interface.

By default, when the terminating router matches a dial string to an outbound POTS dial peer, the router strips off the left-justified digits that explicitly match the destination pattern. The remaining wildcard digits are forwarded to the telephony interface, which connects devices such as a PBX or the PSTN.

Digit stripping is the desired action in some situations. There is no need to forward digits out of a POTS dial peer if it is pointing to a Foreign Exchange Station (FXS) port that connects a telephone or fax machine. When digit stripping is turned off on this type of port, the user will hear tones after answering the call because any unconsumed and unmatched digits are passed through the voice path after the call is answered.

When a PBX or the PSTN is connected through the POTS dial peer, digit stripping is not desired because these devices need additional digits to further direct the call. In these situations, the administrator must assess the number of digits that need to be forwarded for the remote device to correctly process the call. With a VoIP dial peer, all digits are passed across the network to the terminating voice-enabled router.

Digit Collection

- **Step 1:** The router collects digits, one at a time, until it can match an outbound dial peer.
- **Step 2:** After a match is made, the router immediately places the call.
- **Step 3:** No further digits are collected.

Example 1: Dialed string is 5550124.

```
dial-peer voice 1 voip
 destination-pattern 555
 session target ip4:10.18.0.1

dial-peer voice 2 voip
 destination-pattern 5550124
 session target ip4:10.18.0.2
```

Dial peer 1 will match first.
Only the collected digits of 555
will be forwarded.

Example 2: Dialed string is 5550124.

```
dial-peer voice 1 voip
 destination-pattern 555...
 session target ip4:10.18.0.1

dial-peer voice 2 voip
 destination-pattern 5550124
 session target ip4:10.18.0.2
```

Dial peer 2 will match first.
The collected digits of 5550124
will be forwarded.

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-2.21

When a voice call enters the network, the router collects digits as described in the table.

How the Router Collects Digits

Step	Action
1.	The originating router collects dialed digits until it matches an outbound dial peer.
2.	The router immediately places the call and forwards the associated dial string.
3.	The router collects no additional dialed digits.

Example: Digit Collection

The figure demonstrates the impact that overlapping destination patterns have on the call-routing decision. In example 1, the destination pattern in dial peer 1 is a subset of the destination pattern in dial peer 2. The router matches one digit at a time against available dial peers. This means that an exact match will always occur on dial peer 1, and dial peer 2 will never be matched.

In example 2, the length of the destination patterns in both dial peers is the same. Dial peer 2 has a more specific value than dial peer 1, so it will be matched first. If the path to IP address 10.18.0.2 is unavailable, dial peer 1 will be used.

Destination patterns are matched based on the longest explicit number match. Digits collected are dependant on the configured destination pattern. The table describes how different number combinations are matched and collected.

Matching Destination Patterns

Dialed Digits	Destination Pattern	Dialed Digits Collected
5550124	5.....	5550124
5550124	555....	5550124
5550124	555	555
5550124	555T	5550124

In the first row of the table, the destination pattern specifies a seven-digit string. The first digit must be a five, and the remaining six digits can be any valid digits. All seven digits must be entered before the destination pattern is matched.

In the second row, the destination pattern specifies a seven-digit string. The first three digits must be 555, and the remaining four digits can be any valid digits. All seven digits must be entered before the destination pattern is matched.

In the third row, the destination pattern specifies a three-digit string. The dialed digits must be exactly 555. When the user begins to dial the seven-digit number, the destination pattern matches after the first three digits are entered. The router then stops collecting digits and places the call. If the call is set up quickly, the answering party at the other end may hear the remaining four digits as the user finishes dialing the string. After a call is set up, any dual tone multifrequency (DTMF) tones are sent through the voice path and played out at the other end.

In the last row, the destination pattern specifies a variable-length digit string that is at least three digits long. The first three digits must be exactly 555, and the remaining digits can be any valid digits. The "T" tells the router to continue collecting digits until the interdigit timer expires. The router stops collecting digits when the timer expires, or when the user presses the pound (#) key.

Configuring Digit Manipulation

This topic describes digit manipulation and the commands that are used to connect to a specified destination.

Digit Manipulation Commands

- prefix
 - **Dial-peer command**
 - **Adds digits to the front of the dial string before it is forwarded to the telephony interface**
- forward-digits
 - **Dial-peer command**
 - **Controls the number of digits forwarded to the telephony interface**
- num-exp
 - **Global command**
 - **Expands an extension into a full telephone number or replaces one number with another**
- translation-rule
 - **Global and dial-peer command**
 - **Digit translation rules used to manipulate the calling number digits, or ANI, or the called number digits, or DNIS, for a voice call**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2/22

Digit manipulation is the task of adding or subtracting digits from the original dialed number to accommodate user dialing habits or gateway needs. The digits can be manipulated before matching an inbound or outbound dial peer. Here is a list of digit manipulation commands for the **dial-peer** command and their uses:

- **prefix:** This command adds digits to the front of the dial string before it is forwarded to the telephony interface. This occurs after the outbound dial peer is matched, but before digits get sent out of the telephony interface. Use the **prefix** command when the dialed digits leaving the router must be changed from the dialed digits that had originally matched the dial peer. For example, a call is dialed using a 4-digit extension such as 0123, but the call needs to be routed to the PSTN, which requires 10-digit dialing. If the four-digit extension matches the last four digits of the actual PSTN number, you can use the **prefix 902555** command to prepend the six additional digits needed for the PSTN to route the call to 902-555-0123. After the POTS dial peer is matched with the destination pattern of 0123, the **prefix** command prepends the additional digits and the string “9025550123” is sent out of the voice port to the PSTN.

- **forward-digits:** This command specifies the number of digits that must be forwarded to the telephony interface, regardless of whether they match explicitly or with wildcards. This command occurs after the outbound dial peer is matched, but before the digits are sent out of the telephony interface. When a specific number of digits are configured for forwarding, the count is right-justified. For example, the POTS dial peer has a destination pattern configured to match all extensions in the 1000 range (**destination-pattern 1...**). By default, only the last three digits are forwarded to the PBX that is connected to the specified voice port. If the PBX needs all four digits to route the call, you must use the command **forward-digits 4**, or **forward-digits all**, so that the appropriate number of digits are forwarded. To restore the **forward-digits** command to its default setting, use the **default forward-digits** command. Using the **no forward-digits** command specifies that no digits are to be forwarded.
- **num-exp:** The **num-exp** global command expands an extension into a full telephone number or replaces one number with another. The number expansion table manipulates the called number. This command occurs before the outbound dial peer is matched. Therefore, you must configure a dial peer with the expanded number in the destination pattern for the call to go through. The number expansion table becomes useful when the PSTN changes the dialing requirements from 7-digit dialing to 10-digit dialing. In this scenario, you can do one of the following:
 - Make all the users dial all 10 digits to match the new POTS dial peer that is pointing to the PSTN
 - Allow the users to continue dialing the 7-digit number as they have before, but expand the number to include the area code before the 10-digit outbound dial peer is matched

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

- **translation-rule:** Digit translation is a two-step configuration process. First, the translation rule is defined at the global level. Then, the rule is applied at the dial-peer level either as inbound or outbound translation on either the called or calling number. Translation rules manipulate the ANI or DNIS digits for a voice call. Translation rules also convert a telephone number into a different number before the call is matched to an inbound dial peer, or before the outbound dial peer forwards the call. For example, an employee may dial a five-digit extension to reach another employee of the same company at another site. If the call is routed through the PSTN to reach the other site, the originating gateway may use translation rules to convert the 5-digit extension into the 10-digit format that is recognized by the central office (CO) switch.

You can also use translation rules to change the numbering type for a call. For example, some gateways may tag a number with more than 11 digits as an international number, even when the user must dial “9” to reach an outside line. In this case, the number that is tagged as an international number needs to be translated into a national number—without the 9—before it is sent to the PSTN.

As illustrated in this topic, there are numerous ways to manipulate digits at various stages of call completion. The administrator needs to determine which command will be most suitable and the requirements that are necessary for manipulation.

Note To test configured translation rules, you must use the **test translation** command.

Example: Using Digit Manipulation Tools

Here is a sample configuration using the **prefix** command:

```
dial-peer voice 1 pots
destination-pattern 555....
prefix 555
port 1/0/0
```

In the sample configuration using the **prefix** command, the device attached to port 1/0/0 needs all seven digits to process the call. On a POTS dial peer, only wildcard-matched digits are forwarded by default. Use the **prefix** command to send the prefix numbers 555 before forwarding the four wildcard-matched digits.

Here is a sample configuration using the **forward-digits** command:

```
dial-peer voice 1 pots
destination-pattern 555....
forward-digits 7
port 1/0/0
```

In the sample configuration using the **forward-digits** command, the device attached to port 1/0/0 needs all seven digits to process the call. On a POTS dial peer, only wildcard-matched digits are forwarded by default. The **forward-digits** command allows the user to specify the total number of digits to forward.

Here is a sample configuration using the number expansion table (**num-exp**) command:

```
num-exp 2... 5552...
dial-peer voice 1 pots
destination-pattern 5552...
port 1/1/0
```

In the sample configuration using the **num-exp** command, the extension number 2... is expanded to 5552... before an outbound dial peer is matched; for example, the user dials 2401, but the outbound dial peer 1 is configured to match 5552401.

Here is a sample configuration using the **translation-rule** command:

```
translation-rule 5
rule 1 2401 5552401
dial-peer voice 1 pots
translate-outgoing called-number 5
```

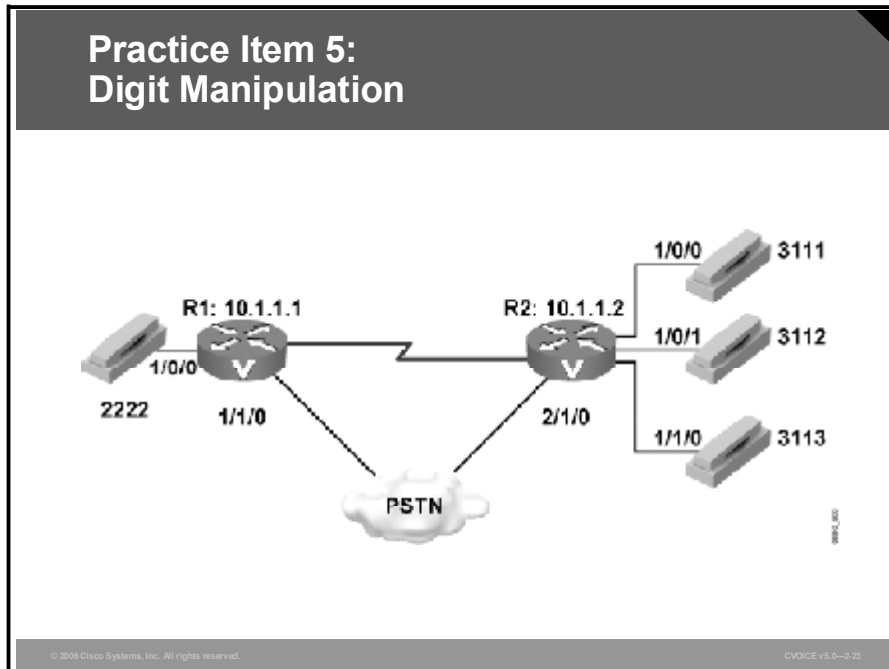
In the sample configuration using the **translation-rule** command, the rule is defined to translate 2401 into 5552401. The dial peer **translate-outgoing called-number 5** command notifies the router to use the globally defined translation rule 5 to translate the number before sending the string out the port. It is applied as an outbound translation from the POTS dial peer.

This example shows a translation rule that converts any called number that starts with 91 and is tagged as an international number into a national number without the 9 before sending it to the PSTN.

```
translation-rule 20
rule 1 91 1 international national
!
!
dial-peer voice 10 pots
destination-pattern 91.....
translate-outgoing called 20
port 1/1:5
forward-digits all
```

Practice Item 5: Digit Manipulation

Assume that all POTS and VoIP dial peers are configured. Create a dial peer to divert calls from R1 to R2 across the PSTN in the event of failure of the VoIP network. Assume that digits must be forwarded to the PSTN, and a prefix of 555 is necessary.



R1

Summary

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

Summary

- A call is segmented into call legs with a dial peer associated with each call leg.
- A call leg is a logical connection between two gateways or routers or between a gateway or router and a telephony endpoint.
- An end-to-end call comprises four call legs: two from the voice router perspective, and two from the destination router perspective.
- A dial peer is an addressable endpoint.
- Cisco voice-enabled routers support POTS dial peers and VoIP dial peers.
- Basic POTS dial-peer configuration consists of defining the dial peer with a tag number and POTS designation, defining the destination pattern, and defining the voice port to which the device is connected.

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-2.24

Summary (Cont.)

- Basic VoIP dial-peer configuration consists of defining the dial peer with a tag number and VoIP designation, defining the destination pattern, and defining the remote voice-enabled router through the session target command.
- Destination patterns can define specific telephone numbers or use wildcards to define a range of numbers.
- If no matching inbound dial peer is configured for a call, the default dial peer is used.
- Inbound dial-peer matching uses the incoming called-number, answer-address, destination-pattern, and port—in that order—to match inbound dial peers.
- Outbound dial-peer matching uses the longest number match in the destination pattern to match an outbound dial peer.

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-2.25

Summary (Cont.)

- **Hunt groups are created when more than one dial peer has the same destination pattern but points to a different voice port or session target.**
 - The **preference** command defines the order in which dial peers are used in a hunt group.
 - The **huntstop** command stops hunting at a specific dial peer if that dial peer is not matched.
 - The **dial-peer hunt** command defines the hunt behavior for all hunt groups on a device.
- **On POTS dial peers, only wildcard-matched digits are forwarded by default.**
- **The prefix and forward-digits commands define how digits are sent out to the voice port.**
- **The num-exp and translation-rule commands define how one number is replaced with another number.**

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-2.28

References

For additional information, refer to this resource:

- *Understanding Inbound and Outbound Dial Peers on Cisco IOS Platforms.*
http://www.cisco.com/warp/public/788/voip/in_out_dial_peers.html

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 2-3: Configuring POTS Dial Peers

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 end-to-end call is established, how many inbound call legs are associated with the call?
- A) one
 - B) two
 - C) three
 - D) four
- Q2) Which dial peers should you configure to complete an end-to-end call?
- A) the inbound dial peers only
 - B) the outbound dial peers only
 - C) one inbound dial peer and one outbound dial peer
 - D) all four dial peers
- Q3) Arrange the steps in the call setup process in the correct order.
- _____ 1. Router 2 creates the inbound voice network call leg and assigns it a Call ID.
 - _____ 2. The POTS call arrives at router 1, and an inbound POTS dial peer is matched.
 - _____ 3. Router 1 creates an outbound voice network call leg and assigns it a Call ID.
 - _____ 4. Router 1 creates an inbound POTS call leg and assigns it a Call ID.
 - _____ 5. The voice network call request arrives at router 2 and an inbound voice network dial peer is matched.
 - _____ 6. Router 2 creates an outbound POTS call leg and assigns it a Call ID.
 - _____ 7. Router 2 uses the dialed string to match an outbound POTS dial peer.
 - _____ 8. At this point, both router 1 and router 2 negotiate voice network capabilities and applications, if required.
 - _____ 9. Router 1 uses the dialed string to match an outbound voice network dial peer.
- Q4) What is the role of the terminating router if the originating router requests nondefault voice capabilities?
- A) The terminating router negotiates with the originating router until the default capabilities are accepted.
 - B) The terminating router reconfigures the ports to meet the requested capabilities.
 - C) The terminating router matches an inbound voice network dial peer that has the requested capabilities.
 - D) The terminating router terminates the call.

- Q5) Which two functions are performed by a POTS dial peer? (Choose two.)
- A) provides an address for the edge network or device
 - B) provides a destination address for the edge device that is located across the network
 - C) routes the call across the network
 - D) identifies the specific voice port that connects the edge network or device
 - E) associates the destination address with the next-hop router or destination router, depending on the technology used
- Q6) The address is configured on each dial peer and is called a _____.
- A) telephone number
 - B) number range
 - C) destination pattern
 - D) call endpoint
- Q7) Which two parameters must be specified on a router that is connected to a telephone? (Choose two.)
- A) voice port
 - B) dial type
 - C) calling plan
 - D) telephone number
- Q8) At which router must you configure a POTS dial peer?
- A) one inbound router on the network
 - B) one outbound router on the network
 - C) one inbound and one outbound router on the network
 - D) each router where edge telephony devices connect to the network
- Q9) Which command is used to specify the address of the terminating router or gateway?
- A) **destination-port**
 - B) **destination-pattern**
 - C) **session target**
 - D) **destination address**
 - E) **dial-peer terminal**
- Q10) Why should the loopback address be used in the **session target** command?
- A) The call fails if the interface goes down.
 - B) The interface will never shut down.
 - C) The call will use an alternate path if the interface shuts down.
 - D) The call will never fail as long as the router is operating.
- Q11) What does a plus sign (+) before the telephone number indicate?
- A) The telephone number must conform to ITU-T Recommendation E.164.
 - B) The number is an extension of a telephone number.
 - C) An additional digit must be dialed before the telephone number.
 - D) The telephone number can vary in length.
- Q12) Which special character in a destination-pattern string is used as a wildcard?
- A) asterisk (*)
 - B) pound sign (#)
 - C) comma (,)
 - D) period (.)
 - E) brackets ([])

- Q13) What happens if there is no matching dial peer for an outbound call?
- A) The default dial peer is used.
 - B) Dial peer 0 is used.
 - C) The POTS dial peer is used.
 - D) The call is dropped.
- Q14) Which four commands represent the default dial-peer configuration for inbound VoIP peers? (Choose four.)
- A) **any codec**
 - B) **no ivr application**
 - C) **vad enabled**
 - D) **no rsvp support**
 - E) **ip precedence 0**
 - F) **destination-pattern .T**
 - G) **default voice port**
- Q15) Which configurable parameter is set for POTS dial peers only?
- A) **answer-address**
 - B) **destination-pattern**
 - C) **incoming called-number**
 - D) **port**
- Q16) In what order does the router attempt to match the called number of the call setup request with a dial-peer attribute?
- _____ 1. **answer-address**
 - _____ 2. **destination-pattern**
 - _____ 3. **incoming called-number**
 - _____ 4. **port**
- Q17) Match the most specific dial-peer configuration to the dialed number.
- A) **dial-peer voice 1 pots**
destination-pattern .T
port 1/0:1
 - B) **dial-peer voice 2 pots**
destination-pattern 555[0-2,5]...
port 1/1/0
 - C) **dial-peer voice 1 pots**
destination-pattern 5553...
port 1/0:1
 - D) **dial-peer voice 1 pots**
destination-pattern 5553216
port 1/0.1
- _____ 1. dialed number is 5551234
 - _____ 2. dialed number is 5553000
 - _____ 3. dialed number is 5553216
 - _____ 4. dialed number is 5554123

- Q18) When the router is matching up with outbound VoIP dial peers, which command is used to forward the call?
- A) **destination-pattern**
 - B) **port**
 - C) **session target**
 - D) **show dialplan number *string***
- Q19) Match the hunt-group commands with their functions.
- A) **preference**
 - B) **dial-peer hunt**
 - C) **show dial-peer voice summary**
 - D) **huntstop**
- _____ 1. shows the current settings for dial-peer hunt
- _____ 2. sets priority for dial peers
- _____ 3. stops dial-peer hunting on the dial peer
- _____ 4. changes the default selection order for hunting through dial peers
- Q20) Which destination has the highest priority?
- A) **dial-peer voice 1 pots**
destination-pattern 5551000
port 1/0/0
preference 0
 - B) **dial-peer voice 1 voip**
destination-pattern 5551200
port 1/1/1
preference 9
 - C) **dial-peer voice 1 pots**
destination-pattern 5551234
port 1/0/0
preference 1
- Q21) By default, what is the first criterion that a router uses to select dial peers in a hunt group?
- A) The router matches the most specific phone number.
 - B) The router matches according to the preference setting.
 - C) The router matches the POTS dial peer first.
 - D) The router matches randomly.
- Q22) When you are configuring a hunt group, which command should you use if the destination pattern of the dial peer is the same for several dial peers?
- A) **dial-peer hunt**
 - B) **huntstop**
 - C) **preference**
 - D) **priority**

Q23) The user is dialing the number 5550124. In the space below each dial peer configuration, specify the digits that are passed out of the telephony interface.

A) **dial-peer voice 1 pots**
destination-pattern 5550124
port 1/0/0

B) **dial-peer voice 2 pots**
destination-pattern 555...
port 1/0/0

C) **dial-peer voice 3 voip**
destination-pattern 555....
session target ipv4: 10.0.0.1

D) **dial-peer voice 4 pots**
destination-pattern 555....
port 1/0/0
no digit-strip

E) **dial-peer voice 5 pots**
destination-pattern 555....
port 1/0/0
forward-digits 6

Q24) What is the default behavior of a terminating router when it matches a dial string to an outbound POTS dial peer?

- A) The router removes the far-left digits that match the destination pattern and forwards the remaining digits.
- B) The router strips off the wildcard digits and forwards the matching digits only.
- C) The router forwards all the digits without attempting a match.
- D) The router does not forward any digits if it cannot match them.

Q25) This **number expansion table** command is used on a dial peer:

```
num-exp 1... 5551...  
!  
dial-peer voice 1 pots  
destination-pattern 5551...  
port 1/1/0
```

If a user dials the number 1825, what numbers will be matched for an outbound dial peer?

- A) 1825
- B) 555
- C) 5551
- D) 5551825

- Q26) A dial peer is configured with the **prefix** command. When are digits added to the front of the dial string?
- A) before the outbound dial peer is matched
 - B) after the outbound dial peer is matched
 - C) after the digits are sent out of the telephony interface
 - D) when the digits are received on the dial peer

Lesson Self-Check Answer Key

Q1) B

Relates to: Dial Peers and Call Legs

Q2) D

Relates to: Dial Peers and Call Legs

Q3)

Step 1 The POTS call arrives at router 1, and an inbound POTS dial peer is matched. (2.)

Step 2 Router 1 creates an inbound POTS call leg and assigns it a Call ID. (4.)

Step 3 Router 1 uses the dialed string to match an outbound voice network dial peer. (9.)

Step 4 Router 1 creates an outbound voice network call leg and assigns it a Call ID. (3.)

Step 5 The voice network call request arrives at router 2 and an inbound voice network dial peer is matched. (5.)

Step 6 Router 2 creates the inbound voice network call leg and assigns it a Call ID. (1.)

Step 7 At this point, both router 1 and router 2 negotiate voice network capabilities and applications, if required. (8.)

Step 8 Router 2 uses the dialed string to match an outbound POTS dial peer. (7.)

Step 9 Router 2 creates an outbound POTS call leg and assigns it a Call ID. (6.)

Relates to: End-to-End Calls

Q4) C

Relates to: End-to-End Calls

Q5) A, D

Relates to: Types of Dial Peers

Q6) C

Relates to: Types of Dial Peers

Q7) A, D

Relates to: Configuring POTS Dial Peers

Q8) D

Relates to: Configuring POTS Dial Peers

Q9) C

Relates to: Configuring VoIP Dial Peers

Q10) B

Relates to: Configuring VoIP Dial Peers

Q11) A

Relates to: Configuring Destination-Pattern Options

- Q12) D
Relates to: Configuring Destination-Pattern Options
- Q13) D
Relates to: Default Dial Peer
- Q14) A, C, D, E
Relates to: Default Dial Peer
- Q15) D
Relates to: Matching Inbound Dial Peers
- Q16) 1. **incoming called-number**
2. **answer-address**
3. **destination-pattern**
4. **port**
Relates to: Matching Inbound Dial Peers
- Q17) 1-B; 2-C; 3-D; 4-A
Relates to: Matching Outbound Dial Peers
- Q18) C
Relates to: Matching Outbound Dial Peers
- Q19) 1-C, 2-A, 3-D, 4-B
Relates to: Configuring Hunt Groups
- Q20) A
Relates to: Configuring Hunt Groups
- Q21) A
Relates to: Configuring Hunt Groups
- Q22) C
Relates to: Configuring Hunt Groups
- Q23) A-None
B-012
C-5550124
D-5550124
E-555012
Relates to: Digit Collection and Consumption
- Q24) A
Relates to: Digit Collection and Consumption
- Q25) D
Relates to: Configuring Digit Manipulation
- Q26) B
Relates to: Configuring Digit Manipulation

Lesson 4

Configuring Voice Port Network Connections

Overview

This lesson explores the uses and applications of various special-purpose connections on Cisco telephony equipment.

Relevance

Integrating Voice over IP (VoIP) technologies to legacy PBXs and public switched telephone networks (PSTNs) often requires voice port configuration for certain connection types. The original design often calls for tie-lines between PBXs. When replacing tie-lines with a VoIP solution, special configuration at the voice port level can emulate the original tie-line design. In many cases, telecommuters require access to PBX services that resemble other extensions of the PBX, regardless of where the telecommuters actually reside. In other instances, telephones, such as lobby customer-service telephones, need to be connected directly to customer service staff. It is important to understand how to provide these services through voice port configuration.

Objectives

Upon completing this lesson, you will be able to correctly configure voice ports for connection types necessary to integrate VoIP technologies with legacy PBXs and PSTN. This ability includes being able to meet these objectives:

- Describe the types and uses of special-purpose connections
- Identify special-purpose **connection** command syntax and options
- Describe how the network establishes PLAR connections
- Describe how the network establishes PLAR OPX connections
- Configure trunk connections
- Describe how the network establishes tie-line connections

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Familiarity with trunk and tie-line concepts
- Familiarity with voice port configuration

Outline

The outline lists the topics included in this lesson.

Outline

- **Overview**
- **Connection Types**
- **Using the connection Command**
- **Configuring PLAR Connections**
- **Configuring PLAR OPX Connections**
- **Configuring Trunk Connections**
- **Configuring Tie-Line Connections**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v6.0-2-2

Connection Types

This topic identifies different special-purpose connection types.

Connection Types

- **PLAR**
 - Associates a voice port directly with a dial peer
- **PLAR-OPX**
 - Extends a PBX connection to a remote location
- **Trunk**
 - Emulates a permanent trunk connection to a PBX
- **Tie-line**
 - Emulates a temporary tie-line trunk to a PBX

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2-3

You can configure voice ports to support special connection requirements. These requirements usually reflect the needs of a specific business environment that must connect to the network in a special way. Here is a list of available connection types and their application:

- **Private line, automatic ringdown (PLAR):** PLAR is an autodialing mechanism that permanently associates a voice port with a far-end voice port, allowing call completion to a specific telephone number or PBX. When the calling telephone goes off hook, a predefined network dial peer is automatically matched, which sets up a call to the destination telephone or PBX. The caller does not hear a dial tone and does not have to dial a number. PLAR connections are widely used in the business world. One common use is to connect stockbrokers with trading floors. Timing is critical when dealing with stock transactions—the amount of time it may take to dial a number and get a connection can be costly in some cases. Another common use is in the travel sector, directly connecting travelers with services. Often, at places like airports, the traveler will see display boards advertising taxi companies, car rental companies, and local hotels. These displays often have telephones that will connect the traveler directly with the service of choice; the device is preconfigured with the telephone number of the desired service. One obvious difference between these telephones and a normal telephone is that they do not have a dial mechanism.

- **PLAR Off-Premises eXtension (OPX):** Most frequently, a PLAR OPX is a PBX extension that is not located on the business site even though it operates as though it is directly connected to the PBX. Company staff can dial an extension and reach the remote telephone as though it were on site. The remote telephone has access to PBX services such as voice mail and extension dialing. This functionality is most often used when onsite staff members turn into telecommuters. Many companies are cutting back on office space in expensive locations and are setting up their staff with home offices. A PLAR OPX connection is configured between the office and the remote site so that the telecommuter can continue to access all the corporate telephony services in the same manner as before. This allows the telecommuter to dial the same extensions to reach other staff, and to have access to long-distance dialing and other voice services via the same calling codes. From the office perspective, onsite staff can reach the telecommuter by dialing the same extension as before. One OPX connection feature is that when a call is being attempted, the voice-enabled router or gateway that takes the call from the PBX or Cisco CallManager will not report a call completion until the far end has answered the call. Without the OPX configuration, the PBX or Cisco CallManager passes the call to the local gateway or router. Then, the gateway or router routes the call to the PSTN. After the PSTN sends ringing to the telephone, the router will report call completion back to the PBX or Cisco CallManager. At this point, the call is completed. The problem is that if the call is not answered, there is no way to reroute the call to the corporate voice-mail server. From the PBX or Cisco CallManager perspective, the call is completed. When you configure the OPX, however, the gateway or router will not report call completion unless the telephone is actually answered.
- **Trunk:** The trunk connection type specifies a connection that emulates a permanent trunk connection between two PBXs, a PBX and a local extension, or some combination of telephony interfaces with signaling passed transparently through the packet data network. A trunk connection remains permanent in the absence of active calls and is established immediately after configuration. The ports on either end of the connection are dedicated until you disable trunking for that connection. If, for some reason, the link between the two voice ports goes down, the virtual trunk reestablishes itself after the link comes back up. This configuration is useful when a permanent connection is desired between two devices. In this scenario, a caller at one end of the trunk connection can pick up the telephone and speak into it without dialing any digits or waiting for call setup. This is analogous to the red telephone to the Kremlin that is depicted in vintage movies. With a trunk connection, there is no digit manipulation performed by the gateway or router. Because this is a permanent connection, digit manipulation is not necessary.
- **Tie-line:** The tie-line connection type specifies a connection that emulates a temporary tie-line trunk to a PBX. Although a tie-line connection is similar to a trunk connection, it is automatically set up for each call and torn down when the call ends. Another difference is that digits are added to the dial string *before* matching an outbound dial peer; for example, if a user were to dial extension 8000, which terminates at a remote office, the voice port is configured with an identifying number for that remote office. If that office ID is the number 7, the digits that are sent to be matched against the outbound dial peer would be 78000. This new five-digit number would be carried across the network to the remote site. At the remote site, the number 7 can be stripped off or, if necessary, passed to the destination device.

Using the connection Command

This topic explains the use and syntax of the **connection** command.

Using the connection Command

Use the connection command in voice-port configuration mode to specify a connection mode for the voice port.

```
router(config-voiceport)#  
connection plar digits
```

- *digits* represent the destination number to be automatically dialed.

```
router(config-voiceport)#  
connection plar-opx digits
```

- *digits* represent the off-premise extension number to be automatically dialed.

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-2.4

Using the connection Command (Cont.)

```
router(config-voiceport)#  
connection trunk digits [answer-mode]
```

- *digits* represent the trunk number to be used to create the virtual trunk across the network.
- *answer-mode* (optional) specifies that the router should wait for an incoming call before establishing the trunk.

```
router(config-voiceport)#  
connection tie-line digits
```

- *digits* represent the tie-line number to be used to create the temporary tie-line.

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-2.5

You configure connection types at the voice port.

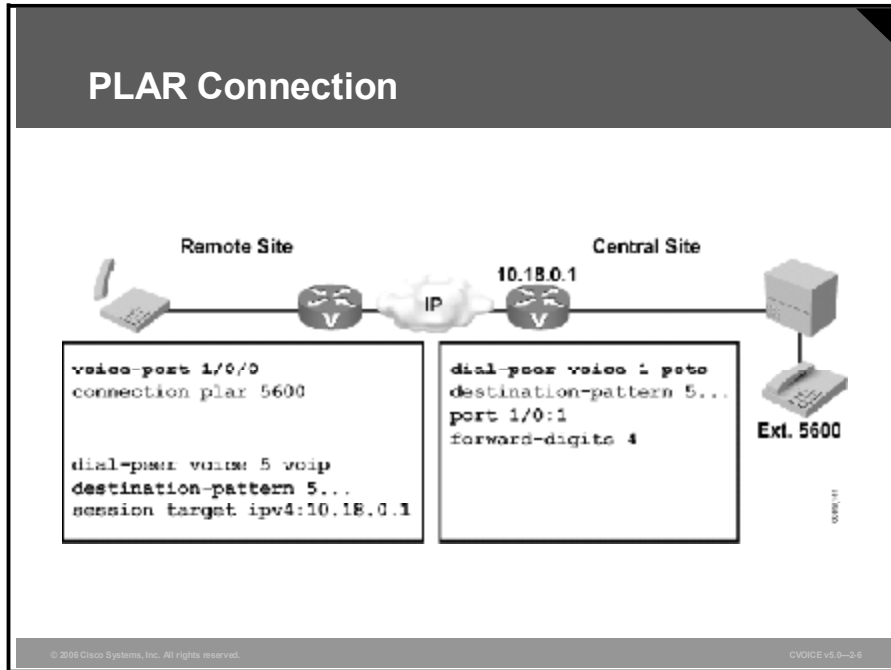
Options for the connection Command

This table describes the options for the **connection** command.

Command Option	Description
<code>connection plar <i>digits</i></code>	■ <i>digits</i> represent the destination number to be automatically dialed.
<code>connection plar-opx <i>digits</i></code>	■ <i>digits</i> represent the off-premise extension number to be automatically dialed.
<code>connection trunk <i>digits</i> [answer-mode]</code>	■ <i>digits</i> represent the trunk number to be used to create the virtual trunk across the network. ■ answer-mode (optional) specifies that the router should wait for an incoming call before establishing the trunk.
<code>connection tie-line <i>digits</i></code>	■ <i>digits</i> represent the tie-line number to be used to create the temporary tie-line.

Configuring PLAR Connections

This topic describes the use and configuration of PLAR connections.

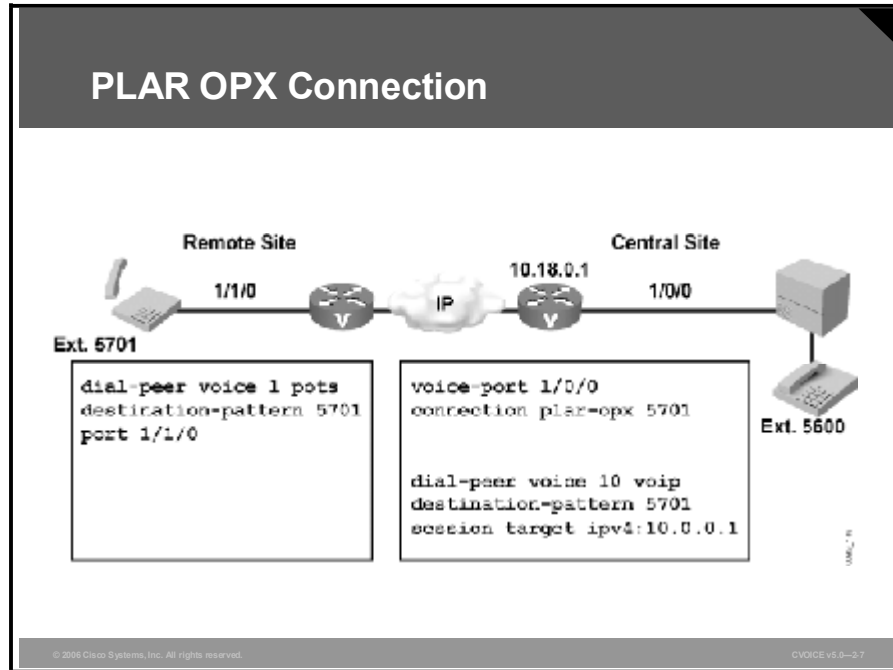


As demonstrated in the figure, these actions must occur to establish a PLAR connection:

1. A user at the remote site lifts the handset.
2. A voice port at the remote site router automatically generates digits 5600 for a dial-peer lookup.
3. The router at the remote site matches digits 5600 to VoIP dial peer 5 and sends the setup message with the digits 5600 to IP address 10.18.0.1 as designated in the **session target** statement.
4. The router at the central site matches received digits 5600 to plain old telephone service (POTS) dial peer 1 and forwards digits 5600 out voice port 1/0:1. At the same time, the router at the central site sends a call setup complete message to the router at the remote site because both the inbound and outbound call legs on the central-site router were processed correctly.
5. The PBX receives digits 5600 and rings the appropriate telephone.

Configuring PLAR OPX Connections

This topic describes the use and configuration of PLAR OPX connections.

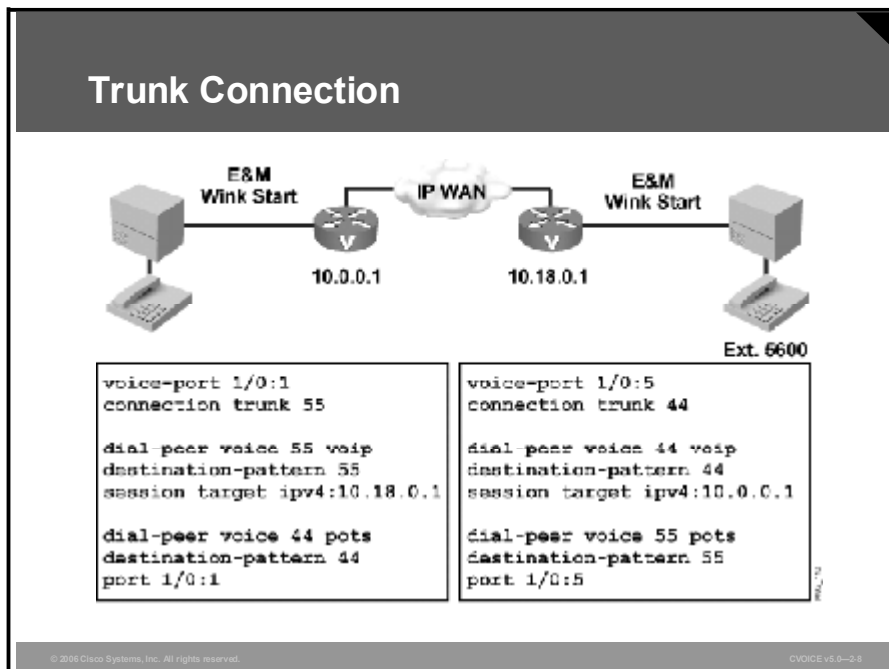


As demonstrated in the figure, these actions must occur to establish a PLAR OPX connection:

1. A user at the central site calls a user at a remote site using the extension 5701.
2. PBX routes the call to the central-site router port 1/0/0, which is configured for PLAR OPX and pointing to extension 5701.
3. The central-site router matches VoIP dial peer 10 and sends a setup message to the corresponding IP address. In the meantime, port 1/0/0 does not respond immediately to the PBX with a seizure or off-hook indication, but waits for the remote site call setup complete message.
4. After the remote router sends the call setup complete message, the central-site router sends a trunk seizure indication to the PBX and opens a voice path.

Configuring Trunk Connections

This topic describes how to configure trunk connections.



As demonstrated in the figure, you must complete this procedure to establish a trunk connection:

1. Use the **connection trunk** command to establish a two-way permanent connection between two voice ports across the IP network.
2. Configure the **connection trunk** parameter on the voice ports connecting the two PBXs and configure the **session target** statement for each IP address.

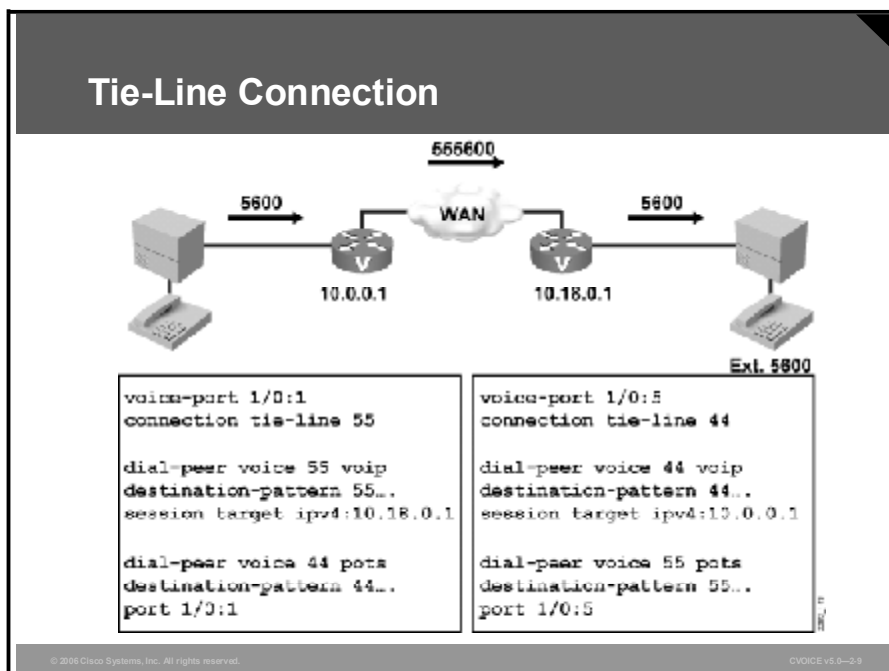
In the example, the router on the left is configured to set up a trunk connection from voice port 1/0:1 to a remote voice-enabled router with the IP address of 10.18.0.1 (the router on the right). This is done by specifying the same number in the **connection trunk** voice port command as in the appropriate dial peer **destination-pattern** command. In this example, the router on the left uses **connection trunk 55**, which matches VoIP dial peer 55. The call is routed to the router on the right, which matches the 55 in a POTS dial peer. The router on the right is also configured to set up a trunk connection from its voice port 1/0:5 to a remote voice-enabled router with the IP address of 10.0.0.1 (the router on the left). The router on the right uses 44 as its connection trunk number. These trunk connections are set up when the routers power on and remain up until the router is powered down or the ports are shut down.

These conditions must be met for VoIP to support virtual trunk connections:

- You must use these voice port combinations:
 - E&M to E&M (same type)
 - Foreign Exchange Station (FXS) to Foreign Exchange Office (FXO)
 - FXS to FXS (with no signaling)
- You must not perform number expansion on the destination-pattern telephone numbers configured for trunk connection.
- You must configure both end routers for trunk connections.

Configuring Tie-Line Connections

This topic describes the use and configuration of tie-lines.



In traditional telephony networks, companies often had dedicated circuits called tie-lines connecting two PBXs. This, in effect, allowed callers at one site to reach callers at the remote site only through that tie-line connection. Now that the IP network is replacing the traditional telephony connection, the two sites are logically “tied” together through the use of the **connection tie-line** command at both sites. Callers at one site can still reach callers at the remote site only, but the call goes over the IP network. The **connection tie-line** command emulates tie-lines between PBXs.

As demonstrated in the figure, you must complete this procedure to establish a tie-line connection:

1. Use the **connection tie-line** command when the dial plan requires the addition of digits in front of any digits dialed by the PBX.
2. Use the combined set of digits to route the call onto the network.
3. The tie-line port waits to collect digits from the PBX.
4. The terminating router automatically strips the tie-line digits.

In the figure, the caller on the left picks up the telephone and dials the four-digit extension, 5600. Because the voice port on the left router is configured for the **connection tie-line** command, the router collects the four digits and prepends the tie-line digits 55 to make a six-digit number, 555600. That number is then matched to a VoIP dial peer and sent to the appropriate IP address. After the call reaches the far-end router, it is matched against a POTS dial peer with the destination pattern “55...”. Because POTS dial peers, by default, forward only wildcard digits, only the four-digit extension 5600 is passed to the PBX.

Summary

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

Summary

- **The connection plar command permanently associates a voice port with a specific telephone number. The voice port does not present a dial tone, but automatically generates the configured number.**
- **The connection plar-opx command provides far-end answer supervision to the local PBX from the originating router. The PBX does not see the call as completed until the far-end router answers.**
- **The connection trunk command establishes a two-way, permanent trunk connection between two PBXs. Supported signaling is E&M-to-E&M, FXS-to-FXO, and FXS-to-FXS.**
- **The connection tie-line command emulates a temporary tie-line trunk to a PBX. A tie-line connection is automatically set up for each call and torn down when the call ends.**

References

For additional information, refer to this resource:

- *Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2.*
(A user ID and password are required to access this site.)
http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ada.html.

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 2-4: Configuring Special-Purpose Connections

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 Cisco IOS command would you use if you want a site ID number to be prepended to the dialed digits before they are trunked across the network?

- A) **connection plar**
- B) **connection plar-opx**
- C) **connection tie-line**
- D) **connection trunk**

Q2) What happens when a dial peer is configured with Cisco IOS command **connection plar**?

- A) The caller hears a dial tone, and the number is automatically dialed.
- B) The caller does not hear a dial tone, and the call is automatically set up.
- C) The caller dials an extension and reaches a telephone on a remote site.
- D) The caller does not hear a dial tone, and the call is set up after dialing.

Q3) The voice port at the remote site is configured with this command:

```
voice-port 1/0/0  
connection plar 5678
```

What is the next step to make a call after the user at the remote site lifts the handset?

- A) The user must dial extension 5678 to make the call.
- B) The telephone will automatically dial 5678, and the user need only dial the extension.
- C) The voice port will automatically generate digits 5678 for a dial-peer lookup.
- D) The voice port has been permanently associated with dial peer 5678, and the call is already established.

Q4) The voice port at the remote site is configured with this command:

```
voice-port 1/0/0  
connection plar-opx 5678
```

What is the next step to make a call after the user at the remote site lifts the handset?

- A) The user must dial extension 5678 to make the call.
- B) The telephone will automatically dial 5678, and the user need only dial the extension.
- C) The voice port will automatically generate digits 5678 for a dial-peer lookup.
- D) The voice port has been permanently associated with dial peer 5678, and the call is already established.

- Q5) Which two conditions are necessary for VoIP to support virtual trunk connections?
(Choose two.)
- A) Both end routers are configured for trunk connections.
 - B) Number expansion is used for the telephone numbers configured for the trunk connection.
 - C) E&M voice ports are connected to E&M voice ports.
 - D) FXO voice ports are connected to FXO voice ports.
 - E) FXS voice ports are connected to FXO voice ports with no signaling.
- Q6) On which POTS voice ports must the **connection trunk** command be configured?
- A) the voice ports connecting the two FXS trunks
 - B) the voice ports connecting the FXS trunk to the FXO trunk
 - C) the voice ports connecting the two PBX trunks
 - D) the voice ports connecting the E&M trunk to the FXS trunk
- Q7) A dial peer is configured with this command:
- ```
voice-port 1/0:1
connection tie-line 35
```
- If the caller dials 7901, what number does the router at the caller end try to match to a dial peer?
- A) 35
  - B) 7901
  - C) 790135
  - D) 357901
- Q8) How do tie-line connections over IP networks differ from tie-line connections over traditional telephony networks?
- A) The calls go over the IP network.
  - B) Callers can dial a shorter number.
  - C) Callers at one site can reach callers at any other site.
  - D) Callers at one site can reach callers at the remote site only.

## Lesson Self-Check Answer Key

- Q1) C  
**Relates to:** Connection Types
- Q2) B  
**Relates to:** Connection Types
- Q3) C  
**Relates to:** PLAR and PLAR OPX
- Q4) C  
**Relates to:** PLAR and PLAR OPX
- Q5) A, C  
**Relates to:** Configuring Trunk Connections
- Q6) C  
**Relates to:** Configuring Trunk Connections
- Q7) D  
**Relates to:** Tie-Line Connections
- Q8) A  
**Relates to:** Tie-Line Connections



## Module 3

---

# VoIP Signaling and Call Control

---

### Overview

To provide voice communication over an IP network, Real-Time Transport Protocol (RTP) sessions are created. These sessions are dynamically created and facilitated by one of several call control procedures. Typically, these procedures also embody mechanisms for signaling events during voice calls and for managing and collecting statistics about the voice calls. This module focuses on three protocols that offer call control support for Voice over IP (VoIP): H.323, the session initiation protocol (SIP), and the Media Gateway Control Protocol (MGCP).

## Module Objectives

Upon completing this module, you will be able to compare centralized and decentralized call control and signaling protocols.

### Module Objectives

- Identify the appropriate call control model for your network
- Describe how H.323 gateways and gatekeepers are used in VoIP networks
- Configure, monitor, and troubleshoot H.323 gateways and gatekeepers
- Configure, monitor, and troubleshoot SIP on a Cisco router
- Configure, monitor, and troubleshoot MGCP on a Cisco router
- Determine the best call control model for your network

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-2

## Module Outline

The outline lists the components of this module.

### Module Outline

- Introducing Signaling and Call Control
- Introducing H.323
- Deploying and Configuring H.323
- Configuring SIP
- Configuring MGCP
- Comparing Call Control Models

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-3

## Lesson 1

---

# Introducing Signaling and Call Control

---

## Overview

Signaling and call control are fundamental to the call establishment, management, and administration of voice communication in an IP network. This lesson discusses the benefits of using signaling and call control and offers an overview of what signaling and call control services provide.

## Relevance

Because signaling and call control are fundamental to Voice over IP (VoIP), you must understand the roles that signaling and call control play in establishing, managing, and administering connections.

## Objectives

Upon completing this lesson, you will be able to identify the appropriate call control model for your network. This ability includes being able to meet these objectives:

- Describe the endpoints and the common control components used in VoIP signaling and call control environments
- Describe VoIP call control protocols, including H.323, SIP, MGCP, H.248/Megaco protocol, SAP, RTSP, and Cisco CallManager
- Explain why the call control gateway must translate signals from different call control models to support end-to-end calls
- Describe the role of call control in establishing RTP sessions and negotiating features during the call setup procedure
- Describe the functions of call control components, including call accounting and administration, call status and CDRs, and address management and admission control

## Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- An understanding of the protocol environment in which VoIP operates

## Outline

The outline lists the topics included in this lesson.

### Outline

- Overview
- VoIP Signaling
- Call Control Models
- Translation Between Signaling and Call Control Models
- Call Setup
- Call Administration and Accounting
- Summary
- Lesson Self-Check

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-2



# VoIP Signaling

In a traditional voice network, call establishment, progress, and termination are managed by interpreting and propagating signals. Transporting voice over an IP internetwork creates the need for mechanisms to support signaling over the IP component of the end-to-end voice path. This topic introduces the components and services provided by VoIP signaling.

## Model for VoIP Signaling and Call Control

- **VoIP signaling components**
  - **Endpoints**
  - **Common control**
- **Common control components**
  - **Call administration**
  - **Accounting**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0-3.3

In the traditional telephone network, a voice call consists of two paths: an audio path carrying the voice and a signaling path carrying administrative information such as call setup, teardown messages, call status, and call progress signals. ISDN data-channel (D-channel) signaling and Common Channel Signaling System 7 (CCSS7) or Signaling System 7 (SS7) are two examples of signaling systems that are used in traditional telephony.

By introducing VoIP into the call path, the end-to-end path involves at least one call leg that uses an IP internetwork. As in a traditional voice call, support for this VoIP call leg requires two paths: a protocol stack that includes Real-Time Transport Protocol (RTP), which provides the audio call leg, and one or more call control models that provide the signaling path.

A VoIP signaling and call control environment model includes endpoints and optional common control components, as follows:

- **Endpoints:** Endpoints are typically simple, single-user devices, such as terminals, that support either a voice process (for example, the Cisco IP Phone application) or a gateway. In either case, the endpoint must be able to participate in signaling with other VoIP endpoints—directly or indirectly—through common control components. The endpoints must also be able to manipulate the audio that is in the audio path. This may involve performing analog-to-digital conversion or converting the format to digital voice so that it takes advantage of compression technology.

Gateways provide physical or logical interfaces to the traditional telephone network. A gateway that is connected digitally to a service provider central office (CO) switch is an example of a gateway providing a physical interface. A gateway that provides access to an interactive response dialog application is an example of a gateway providing a logical interface.

- **Common control:** In some call control models, the common control component is not defined; in others, it is employed optionally. Common control components provide call administration and accounting. These components provide a variety of services to support call establishment, including those listed here:
  - Call status
  - Address registration and resolution
  - Admission control

Typically, the services of the common control components are implemented as applications. These services are colocated in a single physical device, or distributed over several physical devices with standalone endpoints and gateways.

# Call Control Models

This topic describes several call control models and their corresponding protocols.

## Call Control Models

- **H.323**
- **SIP**
- **MGCP**
- **H.248/Megaco protocol**
- **SAP**
- **RTSP**
- **Cisco CallManager**

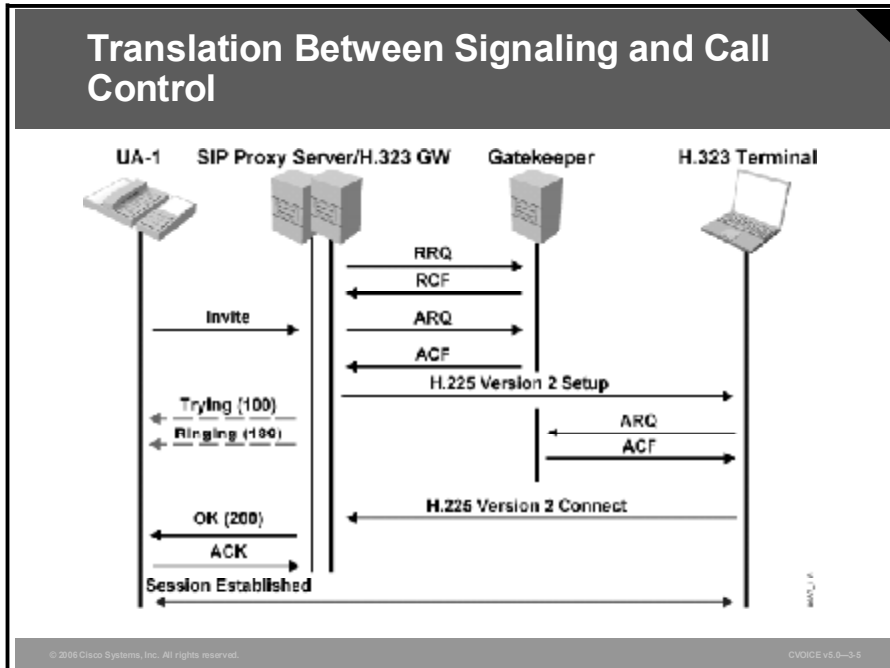
© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-4

These call control models and their corresponding protocols exist or are in development:

- **H.323:** ITU-T Recommendation H.323 describes the architecture to support multimedia communications over networks without quality of service (QoS) guarantees. Originally intended for LANs, H.323 has been adapted for IP.
- **Session initiation protocol (SIP):** SIP is an Internet Engineering Task Force (IETF) RFC 3261 call control model for creating, modifying, and terminating multimedia sessions or calls.
- **Media Gateway Control Protocol (MGCP):** MGCP (IETF RFC 2705) defines a call control model that controls VoIP gateways from an external call control element or call agent.
- **H.248/Megaco protocol:** The Megaco protocol is used in environments in which a media gateway consists of distributed subcomponents, and communication is required between the gateway subcomponents. The Megaco protocol is a joint effort of IETF (RFC 3015) and ITU-T (Recommendation H.248).
- **Session Announcement Protocol (SAP):** SAP (IETF RFC 2974) describes a multicast mechanism for advertising the session characteristics of a multimedia session, including audio and video.
- **Real Time Streaming Protocol (RTSP):** RTSP (IETF RFC 2326) describes a model for controlled, on-demand delivery of real-time audio and video.
- **Cisco CallManager (Skinny Client Control Protocol):** Cisco CallManager is a proprietary Cisco Systems implementation of a call control environment that provides basic call processing, signaling, and connection services to configured devices, such as IP phones, VoIP gateways, and software applications.

# Translation Between Signaling and Call Control Models

When VoIP endpoints support different call control procedures, the calls between the endpoints require cooperation between the originating and terminating procedures. This topic identifies the need for interworking or translation between call control models.



In the traditional telephone network, the individual call legs contributing to an end-to-end call often involve different signaling systems and procedures. In the graphic, an IP Phone is communicating with its SIP proxy server using SIP. However, the IP Phone is also attempting to reach an H.323 endpoint. Because the two VoIP protocols are different, a translation is necessary at the SIP proxy server (namely, an H.323 gateway) to allow the two telephony endpoints to establish a connection.

## Example: Call Control Translation

A call between a residential user and an office worker likely involves a signaling system that is unique to the various call legs that exist between the originator and the destination. In this scenario, the sequence of signaling systems includes these types of signaling:

- Analog signaling (Foreign Exchange Station [FXS] or Foreign Exchange Office [FXO] loop start) to the CO
- CCSS7 between the COs
- ISDN PRI signaling to the PBX
- Proprietary signaling to the desktop telephone

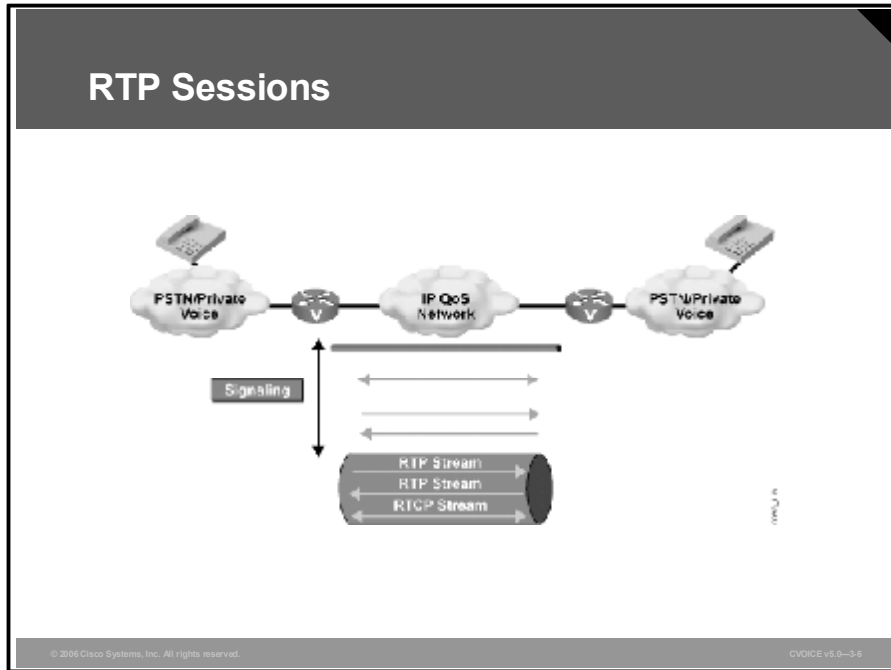
When part of the path is replaced with an IP internetwork, the audio path between the IP endpoints is provided by RTP, and the call control mechanism is based on a call control protocol, such as SIP, H.323, or MGCP.

But what if different call control models represent the endpoints? What if, for example, the originating endpoint uses H.323 and the destination is managed as an SIP endpoint?

To complete calls across the IP internetwork, a call control gateway that recognizes the procedures of *both* call control models is required. In particular, the translating gateway interprets the call setup procedure on the originating side and translates the request to the setup procedure on the destination side. Ideally, this translation is transparent to the endpoints that are involved and results in a single endpoint-to-endpoint audio relationship.

# Call Setup

A fundamental objective of VoIP call control is to initiate communication between VoIP endpoints. This topic discusses the role of call control in establishing RTP sessions and negotiating features during the call setup procedure.

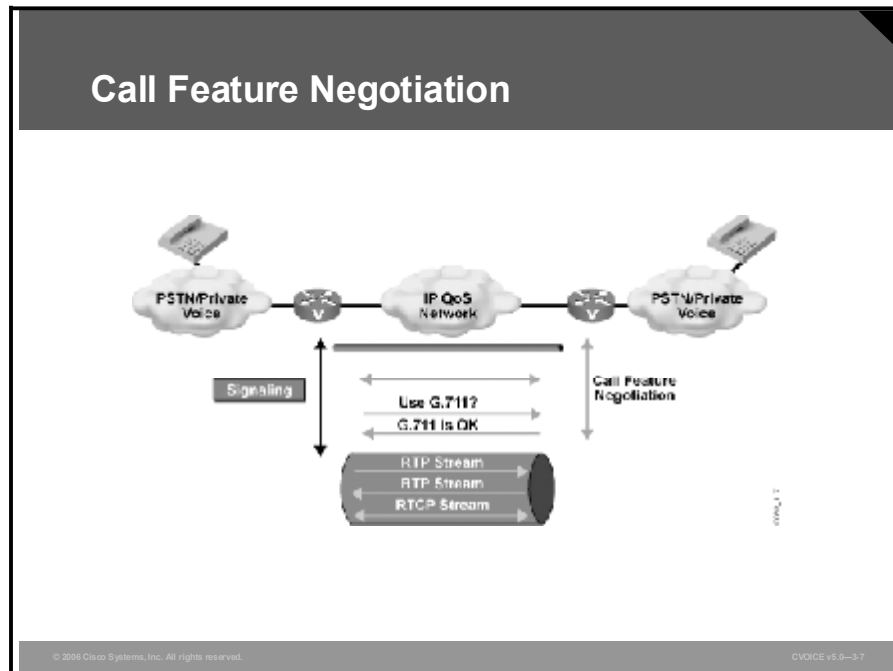


An audio path of a VoIP call leg is dependent on the creation of RTP sessions. These RTP sessions transport voice unidirectionally, so that bidirectional voice uses two RTP sessions. (In principle, if voice is needed in one direction only, as in the case of a recorded announcement or voice mail, only one RTP session is required.) The figure shows RTP sessions being created during call setup.

To create RTP sessions, each endpoint must recognize the IP address and User Datagram Protocol (UDP) port number of its peer. In a limited implementation of VoIP, these values are preprogrammed. However, to be truly scalable, the addresses and port numbers must be recognized dynamically and on demand.

During call setup, call control procedures exchange the IP address and UDP port numbers for the RTP sessions.

## Call Feature Negotiation



Creating the RTP sessions is not the only task of call control during call setup. The endpoints need to establish a bilateral agreement in which the communicating parties discover acceptable call parameters and then agree on the operating parameters of the call. When agreement is not possible, the call is not completed and is dropped.

Here are some examples of call parameters:

- **Coder-decoder (codec):** Each endpoint must share a common format for the voice, or at least must recognize the opposite endpoint choice for voice encoding. This is an example of a mandatory agreement. Not finding a common format is analogous to calling a foreign land and discovering that you are unable to carry on a conversation because the other party speaks a different language.
- **Receive or transmit:** Based on the application, the voice is one-way or two-way. Some endpoints do not meet the requirement for the session because they are designed to handle receive-only traffic or transmit-only traffic when the call requests two-way communication.
- **Multipoint conferences:** Multipoint conferences are the types of conferences and parameters to join.
- **Media type:** The media type is audio, video, or data.
- **Bit rate:** The bit rate represents the throughput requirements.

# Call Administration and Accounting

Call control procedures typically provide support for call administration and accounting. This topic discusses administration and accounting capabilities of call control.

## Call Administration and Accounting

- **Administration**
  - **Monitors call activity**
  - **Monitors resource utilization**
  - **Supports user service requests**
- **Accounting**
  - **Maintains CDRs**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-3.8

Call administration and accounting functions provide optional services for the improved operation, administration, and maintenance of a VoIP environment.

Accounting makes use of the historical information that is usually formatted as Call Detail Records (CDRs). CDRs are useful for cost allocation, and for determining call distribution and service grade for capacity-planning purposes.

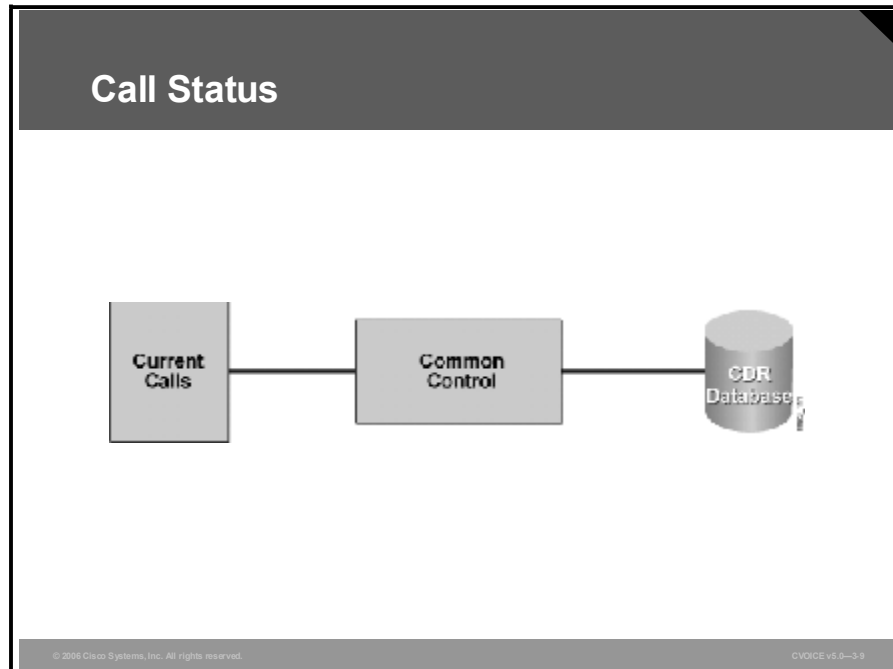
Call administration includes these capabilities:

- **Call status:** Monitoring calls in real time
- **Address management:** Supporting users with services such as address resolution
- **Admission control:** Ensuring that resources are being used effectively



## Call Status and CDRs

Several call control protocols offer dynamic access to the status of calls within the VoIP network. This subtopic discusses the benefits of maintaining call status information and describes where and how call status is used.



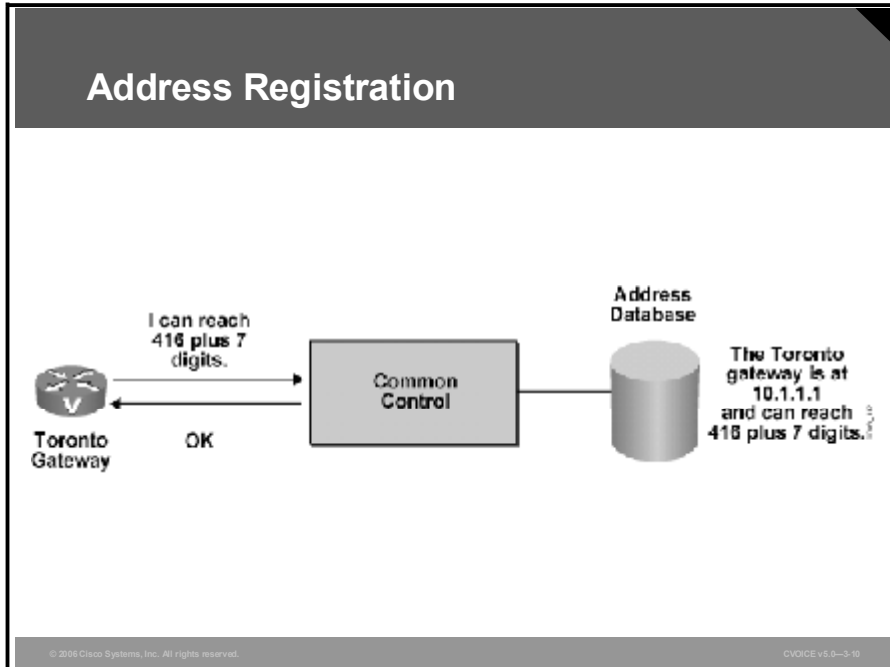
Several of the responsibilities that are assigned to call administration and accounting are dependent on access to current call status information or records of changes in the call status. Call status has both historical and instantaneous (real-time) benefits. CDRs have consequential benefits in terms of distributing costs and planning capacity.

Call status provides an instantaneous view of the calls that are in progress. This view assists other processes (for example, bandwidth management) or assists an administrator with troubleshooting or user support.

CDRs include information about a call start time, duration, origin, destination, and other statistics that may be useful for a variety of purposes. This data is collected as a function of call status.

## Address Management

As an aspect of call administration, call control maintains a database of endpoints and their identifiers. This subtopic discusses how endpoints register their addresses and how these addresses are resolved to IP addresses.

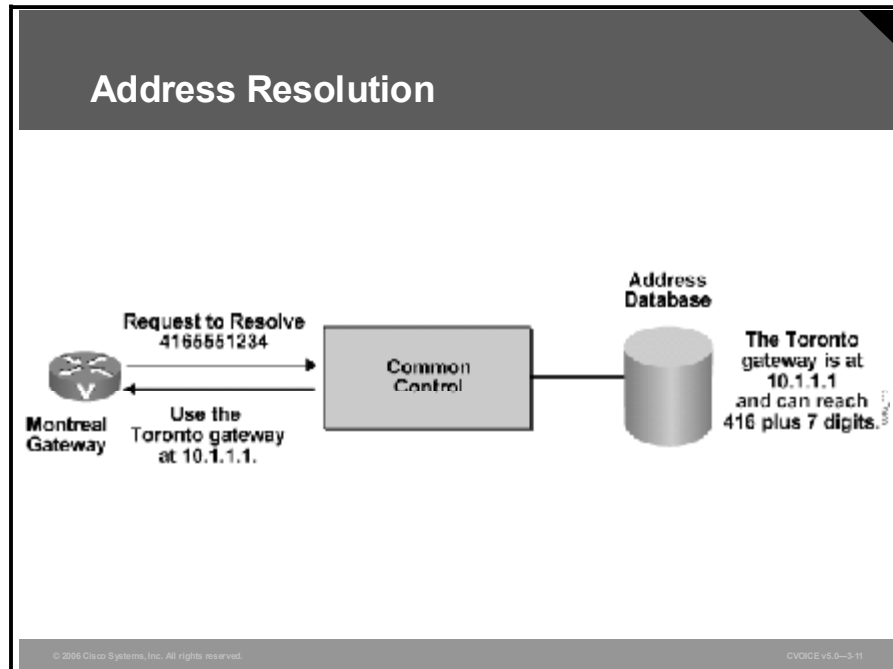


When an endpoint registers with a call control component, it supplies its telephone address or addresses and, if it is a gateway, the addresses of the destinations it can reach. The endpoint provides other information relating to its capabilities. Multiple destinations that are reachable through a gateway are usually represented by a prefix. The use of a prefix allows call control to create a database that associates a telephony-type address, for example, with its corresponding IP address.

In the traditional telephone network, the address of a station is limited to the keys available on a dual-tone multifrequency (DTMF) keypad. In VoIP, an address takes on one of several other formats as well; for example, the address can be a host name or a URL.

## Example: Address Registration

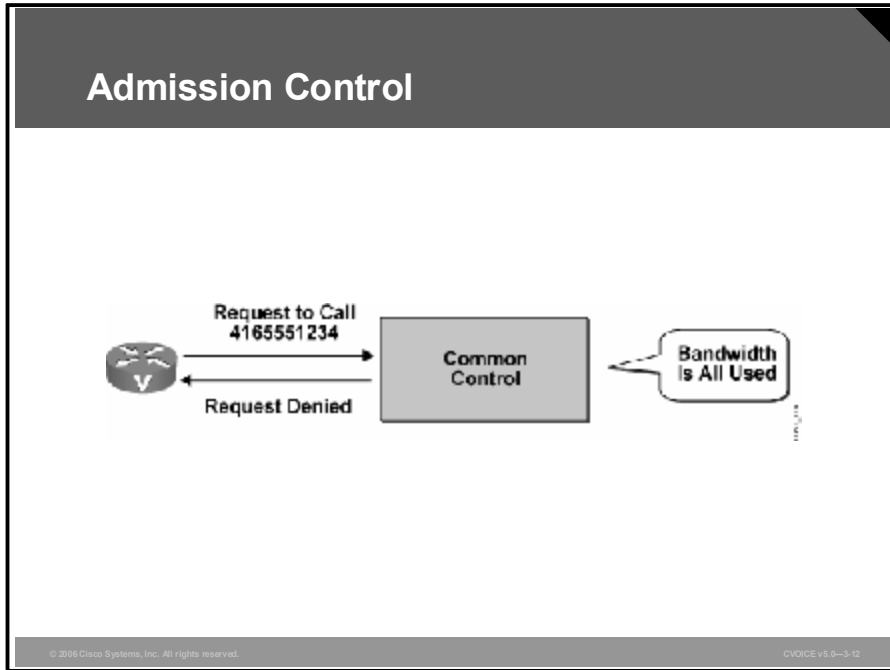
The figure illustrates the Toronto gateway registering its accessibility information. In this example, the gateway informs the common control component that it can reach all telephone numbers in the 416 area. This information is deposited into a database for future reference.



After an address is registered, it can be discovered through address resolution. Address resolution translates a multimedia user address to an IP address so that the endpoints can communicate with each other to establish a control relationship and create an audio path.

## Admission Control

This subtopic discusses how common control and bandwidth management restrict access to the network.



Admission control has at least two aspects: authorization and bandwidth management.

Access to a network should not imply permission to use the resources of the network. Common control limits access to the resources by checking the intentions and credentials of users before authorizing them to proceed.

Bandwidth is a finite resource. Appropriate bandwidth management is essential to maintaining voice quality. Allowing too many voice calls over an IP internetwork results in loss of quality for both new and existing voice calls.

To avoid degrading voice quality, a call control model establishes a bandwidth budget. By using data available from call status, the bandwidth management and Call Admission Control (CAC) functions monitor current bandwidth consumption. Calls may proceed up to the budgeted level, but are refused when the budget has reached its limit. This process is illustrated in the figure.

# Summary

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

## Summary

- **VoIP signaling and call control require endpoints and common control components, such as call administration and accounting.**
- **Protocols used for signaling and call control in VoIP include H.323, SIP, MGCP, Megaco, SAP, RTSP, and Skinny.**
- **Translation between signaling and call control can be achieved at a gateway that implements two or more of the call control capabilities. Translation does not require manipulation of the audio path, only the control path.**
- **One of the main objectives of signaling and call control is to exchange parameters for RTP session establishment and to allow the negotiation of special call features.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-3-10

## Summary (Cont.)

- **Call administration includes call status, address management, and admission control services. Accounting provides call detail records.**
- **Call status provides access to information about calls in progress and facilitates the creation of historical records for cost distribution and network planning.**
- **Address management facilitates registering and locating endpoints.**
- **Access control limits unauthorized access and oversubscription to network resources.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-3-14

## References

For additional information, refer to these resources:

- ITU-T Recommendation H.323
- IETF RFC 3261, *SIP: Session Initiation Protocol*
- IETF RFC 2705, *Media Gateway Control Protocol (MGCP) Version 1.0*

# 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 two examples of signaling systems used in traditional telephony?  
(Choose two.)
- A) cross-channel signaling
  - B) YBTM signaling
  - C) CCSS7
  - D) interswitch signaling
  - E) ISDN D channel
- Q2) Why do endpoints in a VoIP signaling and call control model convert the packet format to digital?
- A) to allow compression technology
  - B) to allow the use of DSPs
  - C) to allow faster transmission
  - D) to reduce errors in transmission
- Q3) What are three examples of VoIP call control protocols? (Choose three.)
- A) SIP
  - B) RSVP
  - C) Megaco protocol
  - D) SAP
  - E) SGBP
- Q4) Match the call control model with its description.
- A) H.323
  - B) MGCP
  - C) H.248
  - D) RTSP
  - E) Skinny Client Control Protocol
- \_\_\_\_\_ 1. a model for controlled, on-demand delivery of real-time audio and video
- \_\_\_\_\_ 2. allows control of VoIP gateways from a call agent
- \_\_\_\_\_ 3. controls communication between the gateway subcomponents
- \_\_\_\_\_ 4. provides basic call processing, signaling, and connection services to configured devices
- \_\_\_\_\_ 5. describes the architecture to support multimedia communications over networks without QoS guarantees
- Q5) On a VoIP network, which protocol carries the audio path?
- A) RTP
  - B) SIP
  - C) H.323
  - D) MGCP

- Q6) When two endpoints using different call control models communicate, which call control function is required at the gateway?
- A) authentication
  - B) compression
  - C) registration
  - D) translation
- Q7) Which two call parameters may be negotiated during call setup? (Choose two.)
- A) codec
  - B) port number
  - C) media type
  - D) E&M requirements
  - E) IP address
- Q8) Which two pieces of information does each endpoint need to recognize to create RTP sessions? (Choose two.)
- A) call agent address
  - B) IP address of its peer
  - C) SMTP protocol used by its peer
  - D) type of firewall traffic being transmitted by its peer
  - E) UDP port number of its peer
- Q9) Which capabilities are NOT included in call administration?
- A) call status
  - B) CDRs
  - C) address management
  - D) admission control
- Q10) Match the call administration and accounting service with its description.
- A) call status
  - B) address management
  - C) admission control
  - D) CDR
- \_\_\_\_\_ 1. ensures that resources are being used effectively
- \_\_\_\_\_ 2. allows determination of call distribution and grade of service
- \_\_\_\_\_ 3. supports users with services such as address resolution
- \_\_\_\_\_ 4. monitors call activity in real time
- Q11) Which two benefits are associated with CDRs? (Choose two.)
- A) bandwidth management
  - B) troubleshooting
  - C) cost distribution
  - D) user support
  - E) capacity planning
- Q12) What is the function of call status?
- A) to estimate the current bandwidth
  - B) to provide CDRs
  - C) to provide authentication information
  - D) to report registered addresses



- Q13) What is the purpose of address resolution?
- A) to obtain the capabilities of an endpoint
  - B) to translate a multimedia user address to an IP address
  - C) to discover routing table information
  - D) to register the telephone numbers that an endpoint can reach
- Q14) How does an endpoint provide information about all the destinations that it can reach?
- A) with a list of all the telephone numbers that it can reach
  - B) with a list of all the IP addresses that it can reach
  - C) with a routing table
  - D) with a prefix
- Q15) What are two aspects of admission control? (Choose two.)
- A) authentication
  - B) authorization
  - C) CDR creation
  - D) bandwidth management
  - E) address resolution
- Q16) What information do the bandwidth management and CAC functions use to monitor bandwidth consumption?
- A) router configuration
  - B) network speed
  - C) CDRs
  - D) call status data

## Lesson Self-Check Answer Key

- Q1) C, E  
**Relates to:** VoIP Signaling
- Q2) A  
**Relates to:** VoIP Signaling
- Q3) A, C, D  
**Relates to:** Call Control Models
- Q4) 1-D  
2-B  
3-C  
4-E  
5-A  
**Relates to:** Call Control Models
- Q5) A  
**Relates to:** Translation Between Signaling and Call Control Models
- Q6) D  
**Relates to:** Translation Between Signaling and Call Control Models
- Q7) A, C  
**Relates to:** Call Setup
- Q8) B, E  
**Relates to:** Call Setup
- Q9) B  
**Relates to:** Call Administration and Accounting
- Q10) 1-C  
2-D  
3-B  
4-A  
**Relates to:** Call Administration and Accounting
- Q11) C, E  
**Relates to:** Call Administration and Accounting
- Q12) A  
**Relates to:** Call Administration and Accounting
- Q13) B  
**Relates to:** Call Administration and Accounting
- Q14) D  
**Relates to:** Call Administration and Accounting

Q15) B, D  
**Relates to:** Call Administration and Accounting

Q16) D  
**Relates to:** Call Administration and Accounting



## Lesson 2

---

# Introducing H.323

---

## Overview

H.323 and its associated ITU-T recommendations represent a distributed environment for establishing voice, video, and data communication in a nonguaranteed quality of service (QoS) network that is typical of an IP internetwork. In addition to describing how to configure H.323, this lesson discusses the features and functions of the H.323 environment, including its components and how they interact. Scalability and survivability issues are also discussed.

## Relevance

An understanding of the features and functions of H.323, its components, and the manner in which the components interact is important to implement a scalable, resilient, and secure H.323 environment.

## Objectives

Upon completing this lesson, you will be able describe how H.323 gateways and gatekeepers are used in Voice over IP (VoIP) networks. This ability includes being able to meet these objectives:

- Explain how H.323 is adopted for use in an IP network environment
- Describe the functions of each component in an H.323 environment
- Identify three types of end-to-end connections that are established with H.323, and list eight types of registration, admission, and status protocol messages that are used to establish these connections
- Provide two scenarios of call flow without a gatekeeper
- Provide a scenario of call flow with a gatekeeper and explain the function of gatekeeper-routed call signaling in the call setup
- Provide a scenario of call flow with multiple gatekeepers and explain how this setup allows scalability
- Describe three types of multipoint conferences supported by H.323

## Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- An understanding of the objectives and principles of signaling and call control in the context of VoIP

## Outline

The outline lists the topics included in this lesson.

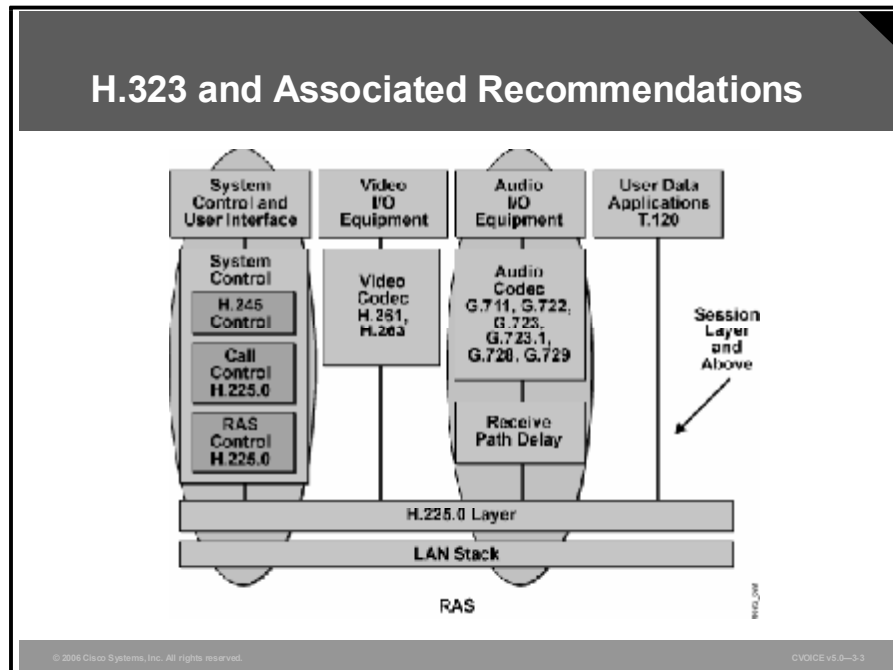
### Outline

- Overview
- H.323 and IP
- Functional Components of H.323
- H.323 Call Establishment and Maintenance
- Call Flows Without a Gatekeeper
- Call Flows with a Gatekeeper
- Call Flows with Multiple Gatekeepers
- Multipoint Conferences
- Summary
- Lesson Self-Check

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-2

## H.323 and IP

This topic describes H.323 and its protocols and explains how H.323 is used in the IP internetwork environment.



Recommendation H.323 describes an infrastructure of terminals, common control components, services, and protocols that are used for multimedia (voice, video, and data) communications. The figure illustrates the elements of an H.323 terminal and highlights the protocol infrastructure of an H.323 endpoint.

H.323 was originally 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, from call establishment to capabilities exchange to network resource availability. H.323 defines these 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 ISDN Q.931 protocol, which allows H.323 to easily interoperate with legacy voice networks, such as the public switched telephone network (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. Here is a description of these functions:

- **Call-signaling function:** The call-signaling 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 (ITU-T Recommendation Q.931). The call-signaling function uses messages formatted according to H.225.0.
- **H.245 control function:** The H.245 control 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.

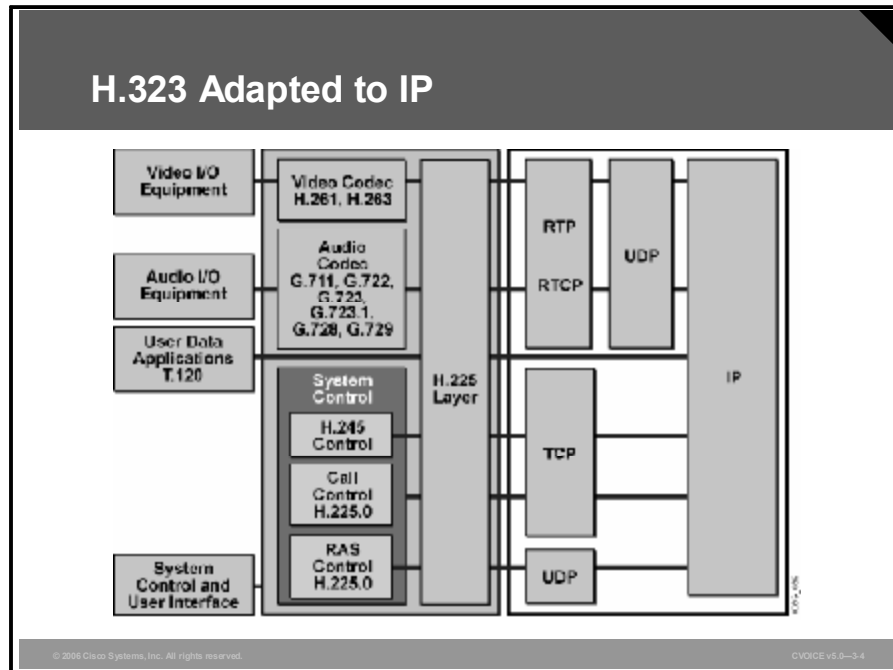
The H.245 control function is responsible for these functions:

- **Logical channel signaling:** Opens and closes the channel that carries the media stream
  - **Capabilities exchange:** Negotiates audio, video, and coder-decoder (codec) capability between the endpoints
  - **Master or responder determination:** Determines which endpoint is master and which is responder; 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:** The RAS signaling function uses a separate signaling channel (RAS channel) to perform registration, admissions, bandwidth changes, status, and disengage procedures between endpoints and a gatekeeper. The RAS signaling function uses messages formatted according to H.225.0.



## Example: H.323 Adapted to IP

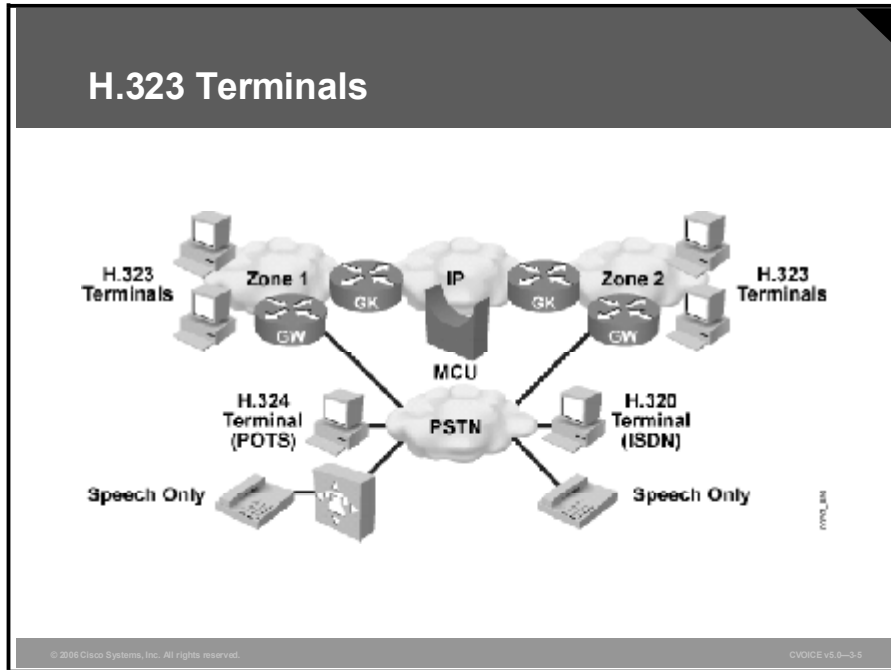
A typical implementation of H.323 goes beyond the original LAN context of H.323. The figure illustrates a specific application of H.323 on an IP internetwork.



Notice that real-time aspects of H.323 rely on User Datagram Protocol (UDP). Both the session-oriented control procedures and the data media type of H.323 use TCP.

# Functional Components of H.323

This topic describes the functional components that make up an H.323 environment.

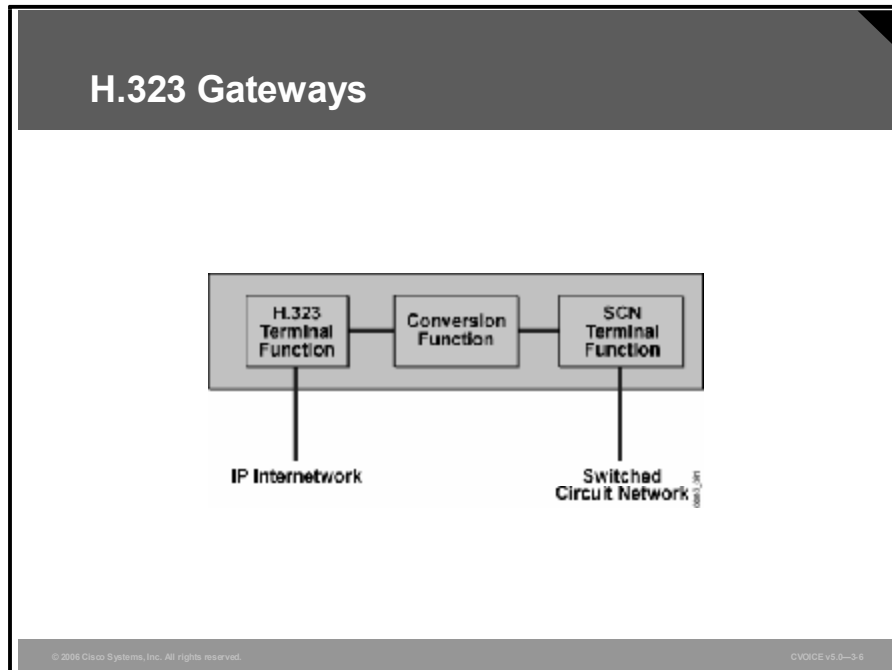


An H.323 terminal is an endpoint that provides real-time voice (and optionally, video and data) communications with another endpoint, such as an H.323 terminal, or multipoint control unit (MCU).

An H.323 terminal must be capable of transmitting and receiving G.711 (a-law and  $\mu$ -law) 64-kbps pulse code modulation (PCM)-encoded voice, and may support other encoded voice formats, such as G.729 and G.723.1.

## H.323 Gateways

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 PSTN or an enterprise voice network. Ideally, the gateway is transparent to both the H.323 endpoint and the SCN-based endpoint.

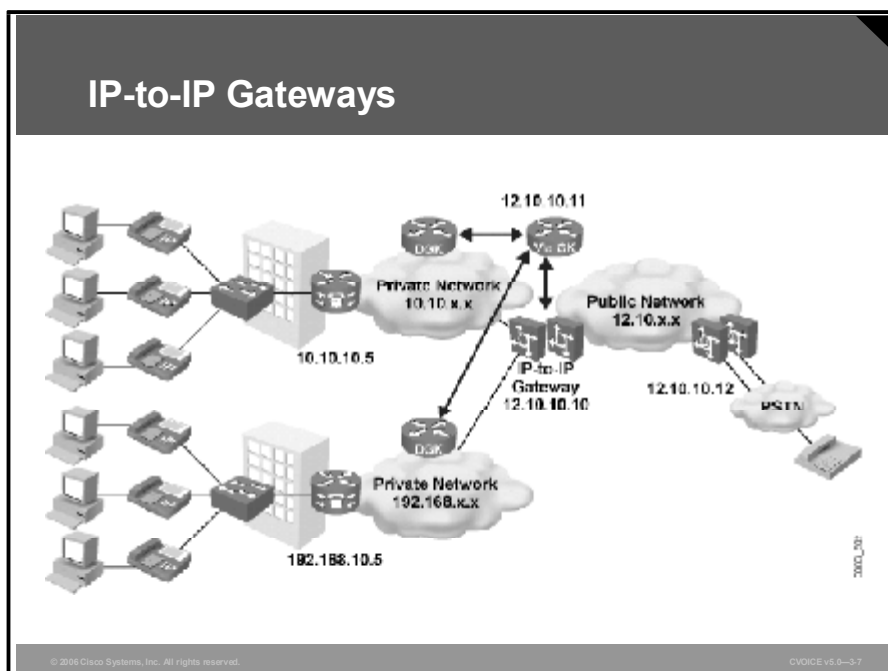


An H.323 gateway performs these services:

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

## IP-to-IP Gateways

This figure shows an example of an IP-to-IP gateway network.

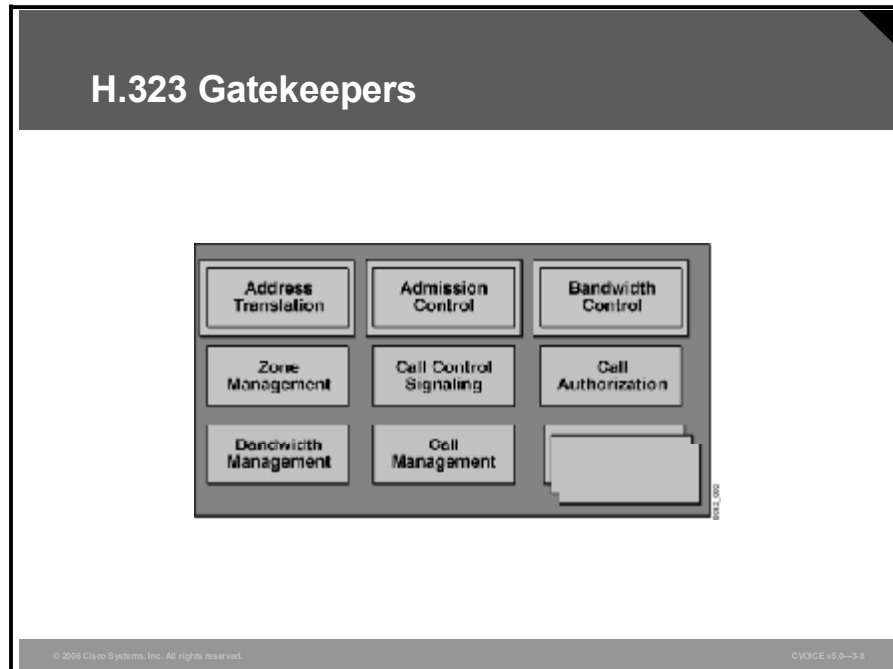


The IP-to-IP gateway facilitates easy and cost-effective connectivity between independent VoIP service provider networks. Some in the industry refer to IP-to-IP gateways as “border elements” or as “session border controllers.” The IP-to-IP gateway provides a network-to-network interface point for billing, security, Cisco CallManager interconnectivity, Call Admission Control (CAC), and signaling interworking. It will perform most of the same functions of a PSTN-to-IP gateway, but will join two VoIP call legs. Media packets can either flow through the gateway and hide the networks from each other, or flow around the IP-to-IP gateway if network security is not of primary importance.

The figure illustrates a basic IP-to-IP gateway network. From the perspective of the private, or customer, networks, the IP-to-IP gateway will appear as a single public address that must be routable on their private networks (in this case, a 12.x.x.x address routable on the 10.10.x.x and 192.168.x.x networks). Care must be taken at the IP-to-IP gateway to ensure that proper routing restrictions are in place to prevent communication directly between the private networks attached to it. Also note that this model works only if no overlapping address schemes are used on the customer networks. Finally, to the hopoff gateways on the public network, all calls will appear to originate from the 12.x.x.x address of the IP-to-IP gateway and not the private addresses on the customer networks. Also note that the gatekeepers shown in the diagram control each zone independently, with the 12.10.10.11 gatekeeper acting as the control point for the public network, and therefore the IP-to-IP gateway.

## H.323 Gatekeepers

An H.323 gatekeeper is an optional component that provides call control support and services to H.323 endpoints. Although a gatekeeper is considered a distinct and optional component, it can be colocated with any other H.323 component.



The scope of endpoints over which a gatekeeper exercises its authority is called a zone. H.323 defines a one-to-one relationship between a zone and a gatekeeper.

When a gatekeeper is included, it must perform these functions:

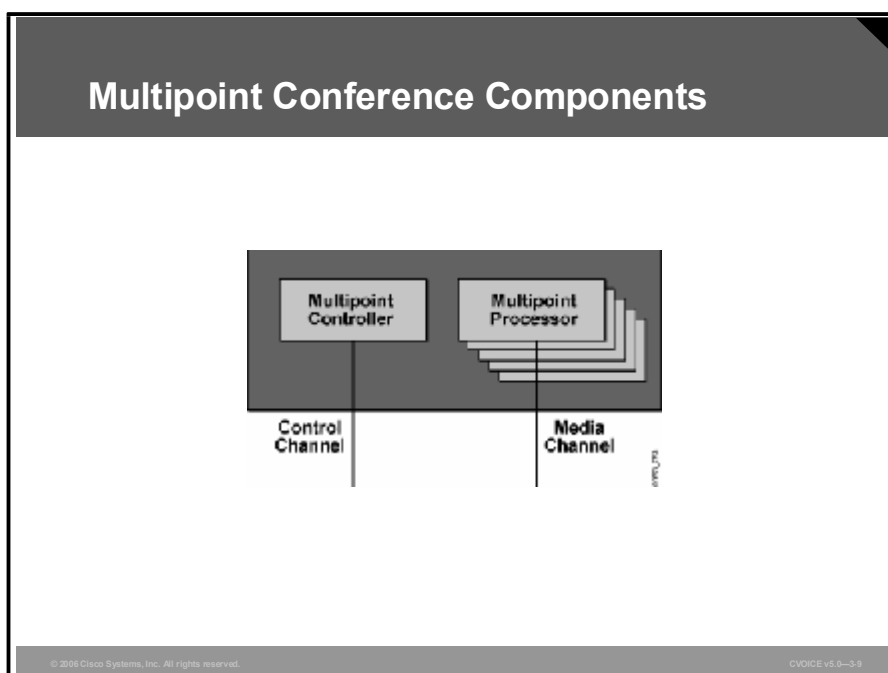
- **Address translation:** Converts an alias address to an IP address
- **Admission control:** Limits access to network resources based on call bandwidth restrictions
- **Bandwidth control:** Responds to bandwidth requests and modifications
- **Zone management:** Provides services to registered endpoints

The gatekeeper may also perform these functions:

- **Call control signaling:** Performs call signaling on behalf of the endpoint (gatekeeper-routed call signaling)
- **Call authorization:** Rejects calls based on authorization failure
- **Bandwidth management:** Limits the number of concurrent accesses to IP internetwork resources (CAC)
- **Call management:** Maintains a record of ongoing calls

## Multipoint Conferences

This subtopic describes the components required for multipoint conferences.



Support for multipoint conferences is provided by these three functional components:

- **MC:** An MC provides the functions that are necessary to support conferences involving three or more endpoints. The MC establishes an H.245 control channel with each of the conference participants. Through the control channel, the MC completes a capability exchange during which the MC indicates the mode of the conference (decentralized or centralized).

An MC is not modeled as a standalone component; it may be located with an endpoint (terminal or gateway), a gatekeeper, or an MCU.

- **Multipoint processor (MP):** An MP adds functionality to multipoint conferences. An MP can receive multiple streams of multimedia input, process the streams by switching and mixing the streams, and then retransmit the result to all or some of the conference members.

Similar to an MC, an MP is not modeled as a standalone component; it resides in an MCU.

- **MCU:** An MCU is modeled as an endpoint that provides support for multipoint conferences by incorporating one MC and zero or more MPs.

An MCU is modeled as a standalone component.

## H.323 Call Establishment and Maintenance

This topic describes possible component scenarios required to establish end-to-end connections and the commands used by the components to establish VoIP calls.

**Component Relationships for Call Establishment and Management**

- **Endpoint (gateway) to endpoint (gateway)**
- **Endpoint (gateway) to gatekeeper**
- **Gatekeeper to gatekeeper**

© 2006 Cisco Systems, Inc. All rights reserved.VOICE vs.0-3-10

Although H.323 is based on the concepts of a distributed call control model, it often embodies centralized call control model concepts. Calls can be established between any of these components:

- **Endpoint to endpoint:** The intelligence of H.323 endpoints allows them to operate autonomously. In this mode of operation, endpoints locate other endpoints through nonstandard mechanisms and initiate direct communication between the endpoints.
- **Endpoint to gatekeeper:** When a gatekeeper is added to the network, endpoints interoperate with the gatekeeper using the RAS channel.
- **Gatekeeper to gatekeeper:** In the presence of multiple gatekeepers, gatekeepers communicate with each other on the RAS channel.

## RAS Messages

Gatekeepers communicate through the RAS channel using different types of RAS messages.

| RAS Messages                           |                              |
|----------------------------------------|------------------------------|
| <b>Gatekeeper Discovery</b>            | <b>Location Request</b>      |
| Gatekeeper Discovery Request (GRQ)     | Location Request (LRQ)       |
| Gatekeeper Confirmation (GCF)          | Location Confirmation (LCF)  |
| Gatekeeper Rejection (GRJ)             | Location Rejection (LRJ)     |
| <b>Terminal/Gateway Registration</b>   | <b>Call Admission</b>        |
| Registration Request (RRQ)             | Admission Request (ARQ)      |
| Registration Confirmation (RCF)        | Admission Confirmation (ACF) |
| Registration Rejection (RRJ)           | Admission Rejection (ARJ)    |
| <b>Terminal/Gateway Unregistration</b> | <b>Disengage</b>             |
| Unregistration Request (URQ)           | Disengage Request (DRQ)      |
| Unregistration Confirmation (UCF)      | Disengage Confirmation (DCF) |
| Unregistration Rejection (URJ)         | Disengage Rejection (DRJ)    |
| <b>Bandwidth Change</b>                | <b>Status Queries</b>        |
| Bandwidth Change Request (BRQ)         | Info Request (IRQ)           |
| Bandwidth Change Confirmation (BCF)    | InfoRequestResponse (IRR)    |
| Bandwidth Change Rejection (BRJ)       | InfoRequestAck (IACK)        |
|                                        | InfoRequestNak (INAK)        |

© 2006 Cisco Systems, Inc. All rights reserved. CVOICEv5.0-3-11

RAS message types include those listed here:

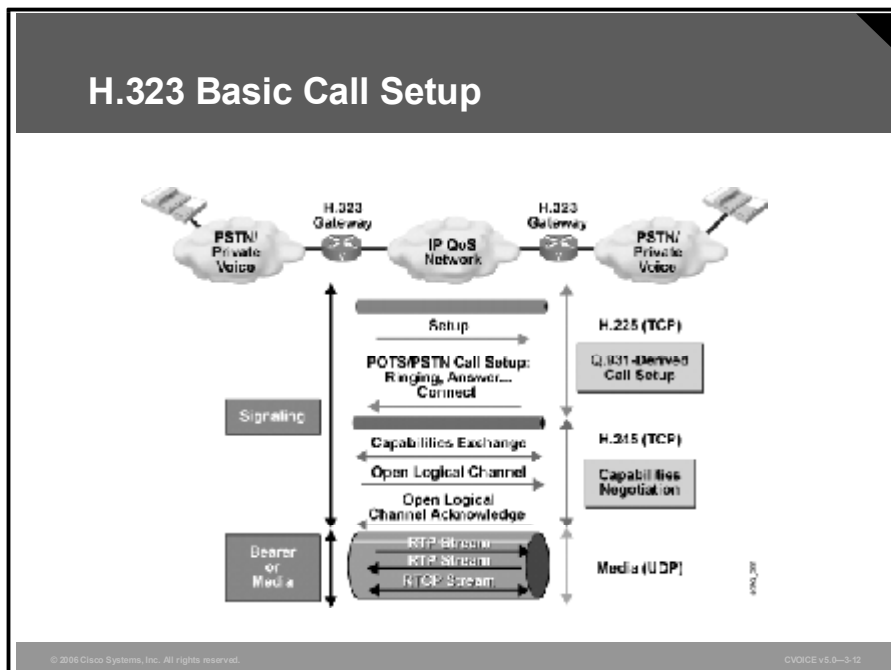
- **Gatekeeper discovery:** An endpoint multicasts a gatekeeper discovery request (GRQ). A gatekeeper may confirm (gatekeeper confirmation [GCF]) or reject (gatekeeper rejection [GRJ]) an endpoint.
- **Terminal and gateway registration:** An endpoint sends a registration request (RRQ) to its gatekeeper to register and provide reachable prefixes. A gatekeeper confirms (registration confirmation [RCF]) or rejects (registration rejection [RRJ]) the registration.
- **Terminal and gateway unregistration:** An endpoint or gatekeeper sends an unregistration request (URQ) to cancel a registration. The responding device confirms (unregistration confirmation [UCF]) or rejects (unregistration rejection [URJ]) the request.
- **Location request:** An endpoint or gatekeeper sends a location request (LRQ) to a gatekeeper. An LRQ is sent directly to a gatekeeper if one is known, or it is multicast to the gatekeeper discovery multicast address. An LRQ requests address translation of an E.164 address and solicits information about the responsible endpoint. The responding gatekeeper confirms (location confirmation [LCF]) with the IP address of the endpoint or rejects the request (location rejection [LRJ]) if the address is unknown.
- **Call admission:** An endpoint sends an admission request (ARQ) to its gatekeeper. The request identifies the terminating endpoint and the bandwidth required. The gatekeeper confirms (admission confirmation [ACF]) with the IP address of the terminating endpoint or rejects (admission rejection [ARJ]) if the endpoint is unknown or inadequate bandwidth is available.
- **Bandwidth change:** An endpoint sends a bandwidth change request (BRQ) to its gatekeeper to request an adjustment in call bandwidth. A gatekeeper confirms (bandwidth confirmation [BCF]) or rejects (bandwidth rejection [BRJ]) the request.



- **Disengage:** When a call is disconnected, the endpoint sends a disengage request (DRQ) to the gatekeeper. The gatekeeper confirms (disengage confirmation [DCF]) or rejects (disengage rejection [DRJ]) the request.
- **Status queries:** A gatekeeper uses an interrupt request (IRQ) to determine the status of an endpoint. In its information request (IRR), the endpoint indicates whether it is on line or off line. The endpoint may also reply that it understands the information request (information request acknowledged [IACK]) or that it does not understand the request (information request not acknowledged [INAK]).

# Call Flows Without a Gatekeeper

This topic describes call setup scenarios without a gatekeeper and provides examples of actual call-flow procedures.



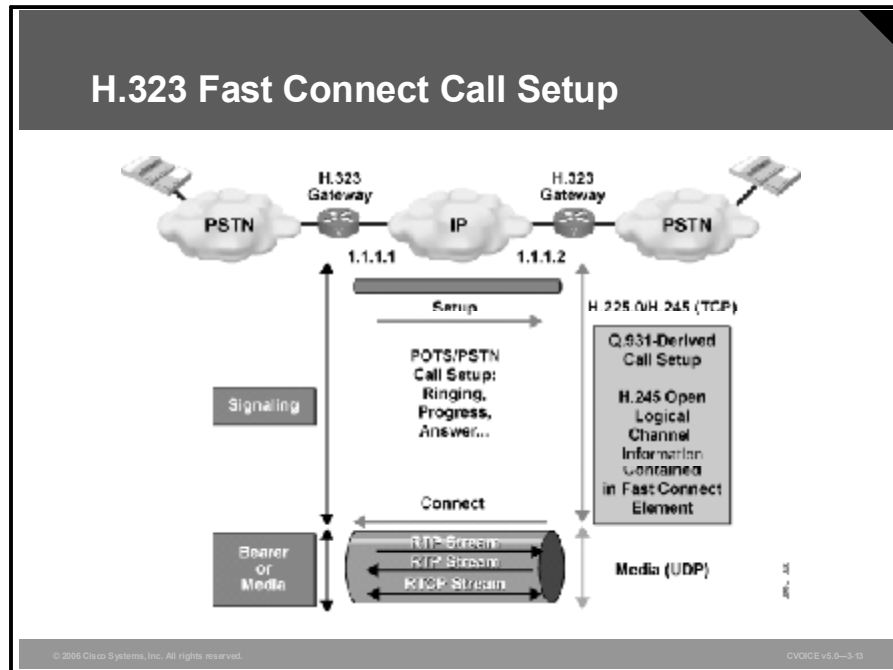
The figure shows an H.323 basic call setup exchange between two gateways. The optional gatekeeper is not present in this example. Although gateways are shown, the same procedure is used when one or both endpoints are H.323 terminals.

The flow procedure without a gatekeeper includes these steps:

1. The originating gateway initiates an H.225.0 session with the destination gateway on registered TCP port 1720. The gateway determines the IP address of the destination gateway internally. The gateway has the IP address of the destination endpoint in its configuration or it knows a Domain Name System (DNS) resolvable domain name for the destination.
2. Call setup procedures based on Q.931 create a call-signaling channel between the endpoints.
3. The endpoints open another channel for the H.245 control function. The H.245 control function negotiates capabilities and exchanges logical channel descriptions.
4. The logical channel descriptions open Real-Time Transport Protocol (RTP) sessions.
5. The endpoints exchange multimedia over the RTP sessions, including exchanging call quality statistics using Real-Time Transport Control Protocol (RTCP).

## H.323 Fast Connect Call Setup

The figure shows an H.323 setup exchange that uses the Fast Connect abbreviated procedure available in version 2 of ITU-T 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:

1. The originating gateway initiates an H.225.0 session with the destination gateway on registered TCP port 1720.
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.
3. Logical channel descriptions open RTP sessions.
4. The endpoints exchange multimedia over the RTP sessions.

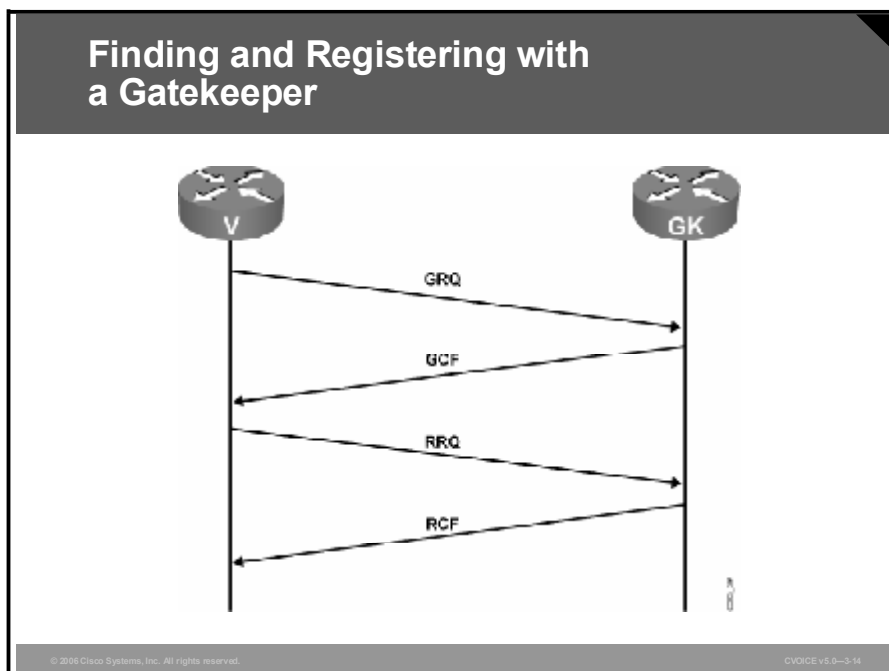
---

**Note** Cisco H.323 voice equipment supports up to version 4 of ITU-T Recommendation H.323 and is backward-compatible to earlier versions.

---

# Call Flows with a Gatekeeper

This topic discusses call setup scenarios with a gatekeeper.



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

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

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

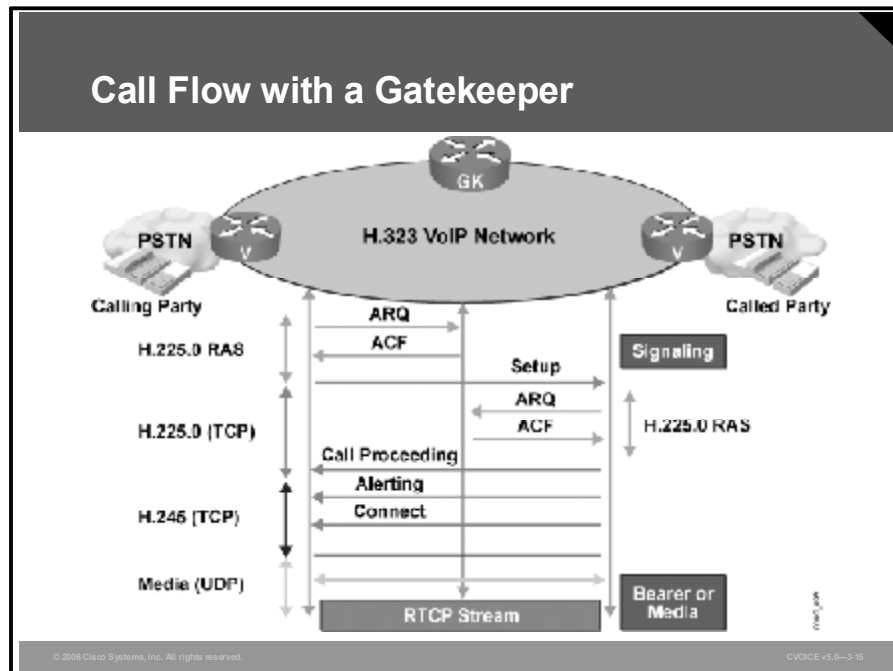
- An endpoint can be preconfigured to recognize the domain name or IP address of its gatekeeper. If configured to recognize the name, an endpoint must have a means to resolve the name to an IP address. A common address resolution technique is the DNS.
- An endpoint can issue a multicast GRQ to the gatekeeper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

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

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

## Call Setup with a Gatekeeper

The exchanges in the figure illustrate the use of a gatekeeper by both endpoints.



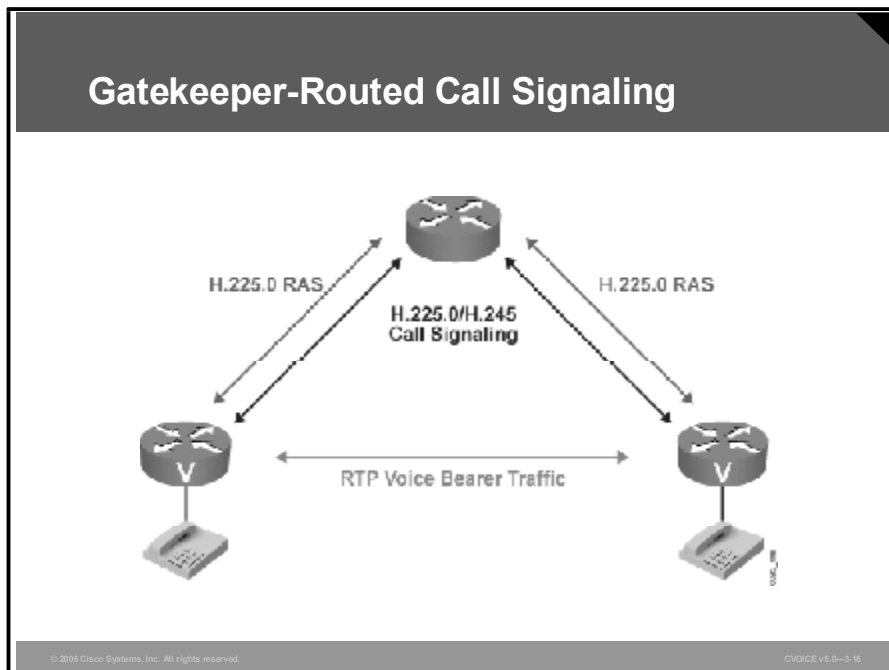
In this example, both endpoints have registered with the same gatekeeper. Call flow with a gatekeeper proceeds as follows:

1. The gateway sends an ARQ to the gatekeeper to initiate the procedure. The gateway is configured with the domain or address of the gatekeeper.
2. The gatekeeper responds to the ARQ with an ACF. In the confirmation, the gatekeeper provides the IP address of the remote endpoint.
3. When the originating endpoint identifies the terminating endpoint, it initiates a basic call setup.
4. Before the terminating endpoint accepts the incoming call, it sends an ARQ to the gatekeeper to gain permission.
5. The gatekeeper responds affirmatively, and the terminating endpoint proceeds with the call setup procedure.

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

## Gatekeeper-Routed Call Signaling

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

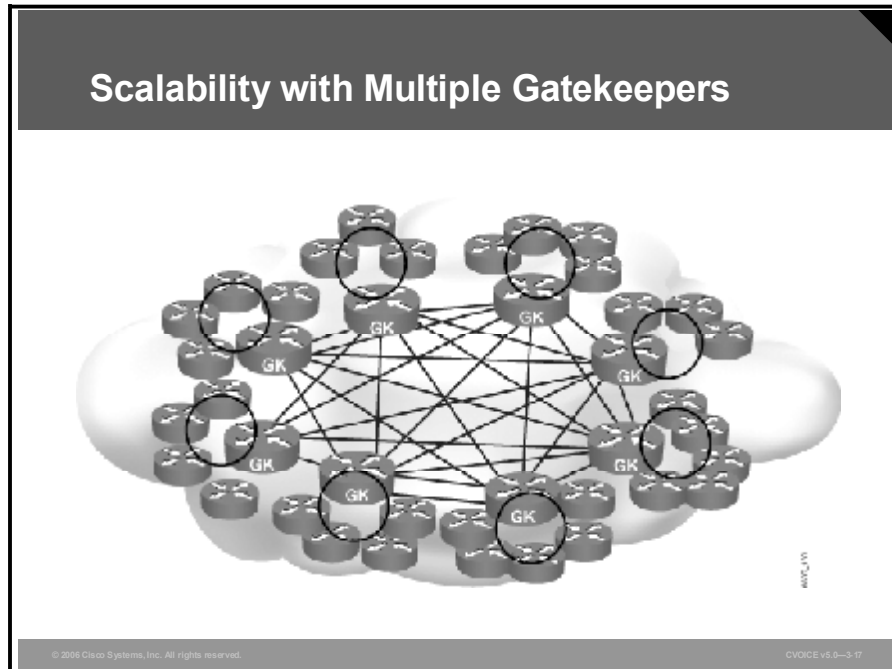


In the previous examples, the call-signaling channel is created from endpoint to endpoint. In some cases, it is desirable to have the gatekeeper represent the other endpoint for signaling purposes. This method is called gatekeeper-routed call signaling. The process for gatekeeper-routed call signaling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

1. The gatekeeper responds to an ARQ and advises the endpoint to perform the call setup procedure with the gatekeeper, not with the terminating endpoint.
2. The endpoint initiates the setup request with the gatekeeper.
3. The gatekeeper sends its own request to the terminating endpoint and incorporates some of the details acquired from the originating request.
4. When a connect message is received from the terminating endpoint, the gatekeeper sends a connect message to the originating endpoint.
5. The two endpoints establish an H.245 control channel between them. The call procedure continues normally from this point.

## Call Flows with Multiple Gatekeepers

By simplifying configuration of the endpoints, gatekeepers aid in building large-scale VoIP networks. As the VoIP network grows, incorporating additional gatekeepers enhances the network scalability. This topic discusses the use of multiple gatekeepers for scalability and illustrates call flow in a multiple gatekeeper environment.



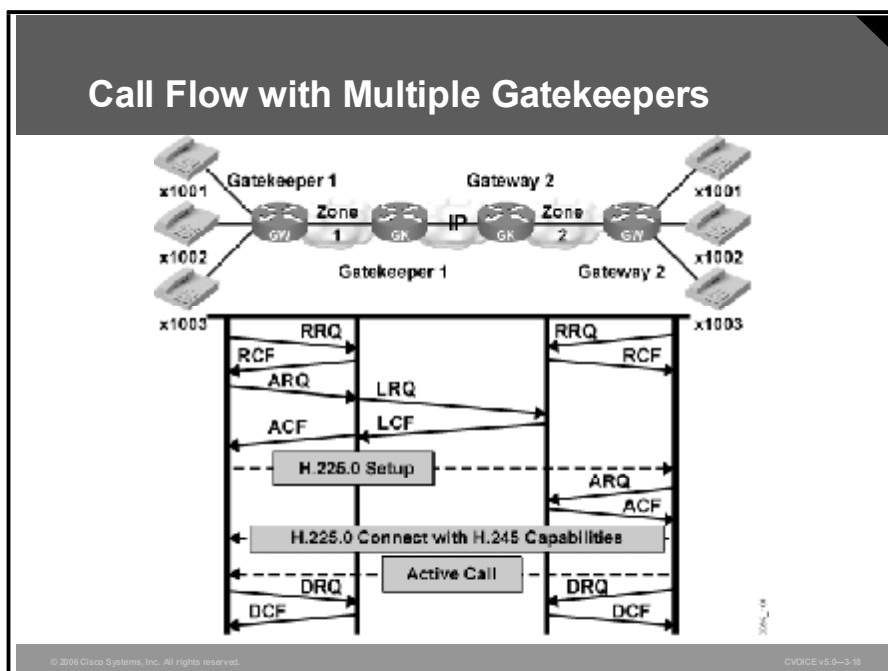
Without a gatekeeper, endpoints must find each other by any means available. This limits the growth potential of the VoIP network. Through the registration and address resolution services of a gatekeeper, growth potential improves significantly.

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

Deploying multiple gatekeepers offers a more scalable and robust environment.

## Call Setup with Multiple Gatekeepers

The figure illustrates a call setup involving two gatekeepers.



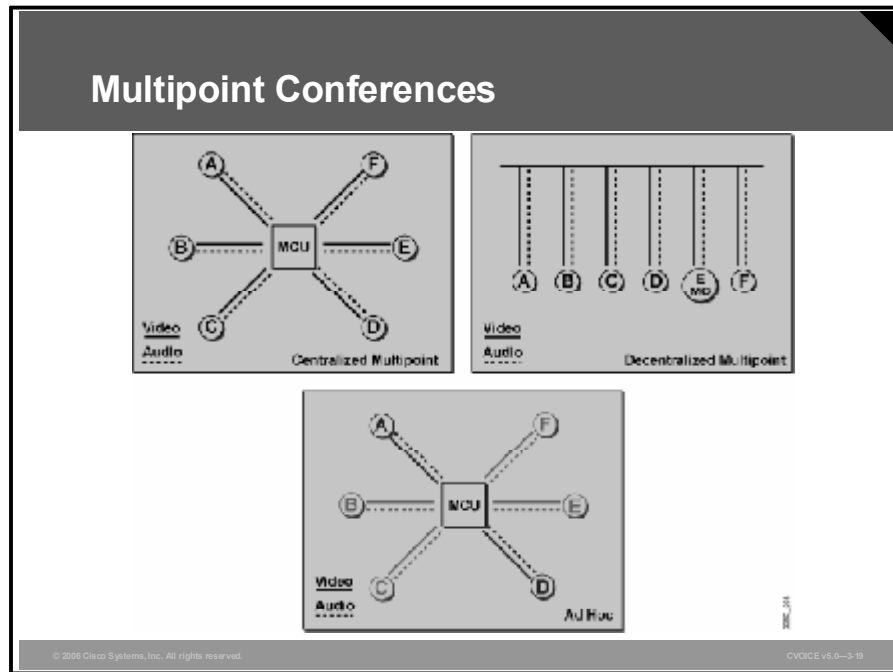
In this example, each endpoint is registered with a different gatekeeper. Notice the changes in the following call setup procedure:

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



# Multipoint Conferences

H.323 defines three types of multipoint conferences: centralized, distributed, and ad hoc. H.323 also defines a hybrid of the first two. This topic describes the multipoint conference control components used to support these conferences.



All types of multipoint conferences rely on a single MC to coordinate the membership of a conference. Each endpoint has an H.245 control channel connection to the MC. Either the MC or the endpoint initiates the control channel setup. H.323 defines the following three types of conferences:

- **Centralized multipoint conference:** The endpoints must have their audio, video, or data channels connected to an MP. The MP performs mixing and switching of the audio, video, and data, and if the MP supports the capability, each endpoint can operate in a different mode.
- **Distributed multipoint conference:** The endpoints do not have a connection to an MP. Instead, endpoints multicast their audio, video, and data streams to all participants in the conference. Because an MP is not available for switching and mixing, any mixing of the conference streams is a function of the endpoint, and all endpoints must use the same communication parameters.

To accommodate situations in which two streams (audio and video) would be handled by the different multipoint conference models, H.323 defines a "hybrid." A hybrid describes a situation in which the audio and video streams are managed by a single H.245 control channel with the MC, but where one stream relies on multicast (according to the distributed model) and the other uses the MP (as in the centralized model).

- **Ad hoc multipoint conference:** Any two endpoints in a call can convert their relationship into a point-to-point conference. If neither of the endpoints has a colocated MC, the services of a gatekeeper are used. When the point-to-point conference is created, other endpoints become part of the conference by accepting an invitation from a current participant, or the endpoint can request to join the conference.

# Summary

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

## Summary

- **H.323 includes recommendations for capabilities exchange, call setup, and call routing.**
- **An H.323 environment includes terminals, gateways, gatekeepers, and components for multipoint conferences.**
- **Although H.323 is based on a distributed call control model, it often uses some components of a centralized call control model to enhance scalability.**
- **When a gatekeeper is used in an H.323 design, RAS signaling is used for communication with endpoints and other gatekeepers.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-3.20

## Summary (Cont.)

- **IP-to-IP gateways facilitate the connection between two VoIP networks.**
- **A basic or Fast Connect H.323 call setup does not require a gatekeeper.**
- **Adding a gatekeeper to the H.323 network enhances scalability by centralizing call address resolution.**
- **Multiple gatekeepers can be used to build large VoIP networks.**
- **H.323 defines three types of multipoint conferences: centralized, decentralized, and ad hoc.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-3.21

## References

For additional information, refer to these resources:

- ITU-T Recommendation H.323 (version 4).  
<http://www.itu.int/rec/recommendation.asp?type=items&lang=E&parent=T-REC-H.323-200011-S>.
- *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).
- *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2*.  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_command\\_reference\\_book09186a0080080c8b.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080080c8b.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) Which two tasks are performed by the RAS signaling function of H.225.0? (Choose two.)
- A) performs bandwidth changes
  - B) transports audio messages between endpoints
  - C) performs disengage procedures between endpoints and a gatekeeper
  - D) allows endpoints to create connections between call agents
  - E) defines call setup procedures based on ISDN call setup
- Q2) Match the H.245 control function with its description.
- A) logical channel signaling
  - B) capabilities exchange
  - C) master/slave determination
  - D) mode request
- \_\_\_\_\_ 1. opens and closes the channel that carries the media stream
- \_\_\_\_\_ 2. requests a change in capability of the media stream
- \_\_\_\_\_ 3. negotiates audio, video, and codec capability between the endpoints
- \_\_\_\_\_ 4. is used to resolve conflicts during the call
- Q3) Which H.323 component can be colocated with another H.323 component?
- A) H.323 terminal
  - B) H.323 gateway
  - C) H.323 gatekeeper
  - D) multipoint control unit
- Q4) What are the functions of an H.323 gateway?
- A) converts an alias address to an IP address
  - B) responds to bandwidth requests and modifications
  - C) transmits and receives G.711 PCM-encoded voice
  - D) performs translation between audio, video, and data formats
  - E) receives and processes multiple streams of multimedia input
- Q5) In H.323 call establishment, which channel do endpoints use to communicate with the gatekeeper?
- A) B channel
  - B) RAS channel
  - C) forward channel
  - D) in-band control channel
- Q6) Which RAS message does a gatekeeper use to determine the status of an endpoint?
- A) ARQ
  - B) IRQ
  - C) LRQ
  - D) RRQ
  - E) URQ

- Q7) Put in the correct order the steps involved in H.323 basic call setup without a gatekeeper.
- A) Call setup procedures based on Q.931 create a call-signaling channel between the endpoints.
  - B) The H.245 control function negotiates capabilities and exchanges logical channel descriptions.
  - C) The gateway determines the IP address of the destination gateway internally.
  - D) The logical channel descriptions open RTP sessions.
  - E) The endpoints open another channel for the H.245 control function.
  - F) The originating gateway initiates an H.225.0 session with the destination gateway on registered TCP port 1720.
  - G) The endpoints exchange multimedia over the RTP sessions.
- \_\_\_\_\_ 1. Step 1
- \_\_\_\_\_ 2. Step 2
- \_\_\_\_\_ 3. Step 3
- \_\_\_\_\_ 4. Step 4
- \_\_\_\_\_ 5. Step 5
- \_\_\_\_\_ 6. Step 6
- \_\_\_\_\_ 7. Step 7
- Q8) How does the abbreviated call setup procedure in version 2 of ITU-T Recommendation H.323 provide fast setup?
- A) The gateway knows a DNS-resolvable domain name for the destination.
  - B) Endpoints use a separate channel for H.245 control functions to speed up signaling.
  - C) Capability exchange and logical channel assignments are completed in one round trip.
  - D) Endpoints and gateways use the same call control model so that no translation is required.
- Q9) In gatekeeper-routed call signaling, what is the role of the gatekeeper?
- A) The gatekeeper establishes an H.245 control channel with both endpoints.
  - B) The gatekeeper performs call setup, call function, and call control functions.
  - C) The gatekeeper represents the other endpoint for call signaling only.
  - D) The gatekeeper passes on the request from the originating endpoint to the terminating endpoint.
- Q10) What information does the gatekeeper include in the ACF message?
- A) the IP address of the remote endpoint
  - B) the ARQ from the originating endpoint
  - C) the call setup request from the gateway
  - D) network statistics

- Q11) Which two gatekeeper services contribute to scalability of a network? (Choose two.)
- A) address resolution
  - B) authentication
  - C) call control
  - D) call routing
  - E) call signaling
  - F) registration
- Q12) Which gatekeeper in a multiple gatekeeper call flow allows the remote endpoint to accept the incoming call?
- A) the gatekeeper with which the originating endpoint is associated
  - B) the gatekeeper with which the remote endpoint is associated
  - C) the gatekeeper that first received the ARQ
  - D) the gatekeeper that is available to set up the call
- Q13) How are audio and video streams managed in hybrid multipoint conferences?
- A) the audio and video streams use separate control channels
  - B) one stream relies on multicast and the other stream uses the MP
  - C) the audio, video, and data are mixed and switched by the MP
  - D) the audio, video, and data streams are multicast to all conference participants
- Q14) In which type of multipoint conference can two endpoints convert to a point-to-point conference?
- A) centralized
  - B) distributed
  - C) ad hoc
  - D) hybrid

## Lesson Self-Check Answer Key

- Q1) A, C  
**Relates to:** H.323 and IP
- Q2) 1-A  
2-D  
3-B  
4-C  
**Relates to:** H.323 and IP
- Q3) C  
**Relates to:** Functional Components of H.323
- Q4) D  
**Relates to:** Functional Components of H.323
- Q5) B  
**Relates to:** H.323 Call Establishment and Maintenance
- Q6) B  
**Relates to:** H.323 Call Establishment and Maintenance
- Q7) 1-F  
2-C  
3-A  
4-E  
5-B  
6-D  
7-G  
**Relates to:** Call Flows Without a Gatekeeper
- Q8) C  
**Relates to:** Call Flows Without a Gatekeeper
- Q9) C  
**Relates to:** Call Flows with a Gatekeeper
- Q10) A  
**Relates to:** Call Flows with a Gatekeeper
- Q11) A, F  
**Relates to:** Call Flows with Multiple Gatekeepers
- Q12) B  
**Relates to:** Call Flows with Multiple Gatekeepers
- Q13) B  
**Relates to:** Multipoint Conferences
- Q14) C  
**Relates to:** Multipoint Conferences



## Lesson 3

---

# Deploying and Configuring H.323

---

## Overview

Gateways and gatekeepers each provide specific features and functionality to the Voice over IP (VoIP) network. This lesson discusses the configuration of each device type to enable the use of those features and to enable the appropriate communication between device types. Reliability is critical for success in a voice network. This lesson discusses strategies that are used to provide fault tolerance in the voice network. The lesson also discusses the steps necessary to monitor and troubleshoot the VoIP network, as required.

## Relevance

Understanding how to configure gateway and gatekeeper devices within the context of Cisco H.323 design is important to implement a functional, scalable, and resilient H.323 environment.

## Objectives

Upon completing this lesson, you will be able to configure, monitor, and troubleshoot H.323 gateways and gatekeepers. This ability includes being able to meet these objectives:

- Describe design strategies used to provide reliability in an H.323 environment
- Describe how calls are set up when an H.323 proxy server is used
- Describe how Cisco provides support for all the H.323 components
- Configure gateways to interoperate with a gatekeeper
- Configure gatekeepers in a single-zone, single-gatekeeper scenario and in a two-zone, two-gatekeeper scenario
- Monitor H.323 gateways and gatekeepers

## Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- An understanding of the features and functions of gateways and gatekeepers

## Outline

The outline lists the topics included in this lesson.

### Outline

- **Overview**
- **Robust Design**
- **H.323 Proxy Server**
- **Cisco Implementation of H.323**
- **Configuring H.323 Gateways**
- **Configuring H.323 Gatekeepers**
- **Monitoring and Troubleshooting**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3.2

# Robust Design

Maintaining high availability in an H.323 environment requires a design that accommodates failure of a critical component. This topic describes strategies for maintaining VoIP service.

## Survivability Strategies

**H.323 replication strategies include the following:**

- **HSRP**
- **VRRP**
- **Gateway preconfigured for two gatekeepers or for multicast discovery**
- **Multiple gatekeepers configured for the same prefix**
- **Multiple gateways configured for the same prefix**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v9.0-3-3

In any environment that depends on common control components, the vulnerability of the environment is directly proportional to the probability of a common control component failure. In a classical telephone application, fault tolerance is accommodated by incorporating extra common control technology. One strategy replicates all critical components. This expensive approach is often replaced with the more cost-effective solution of “ $n$  out of  $n + 1$ ” redundancy; a single spare component is available to step in when any one of the active  $n$  components fails. The essential part of either strategy is the replication of key components.

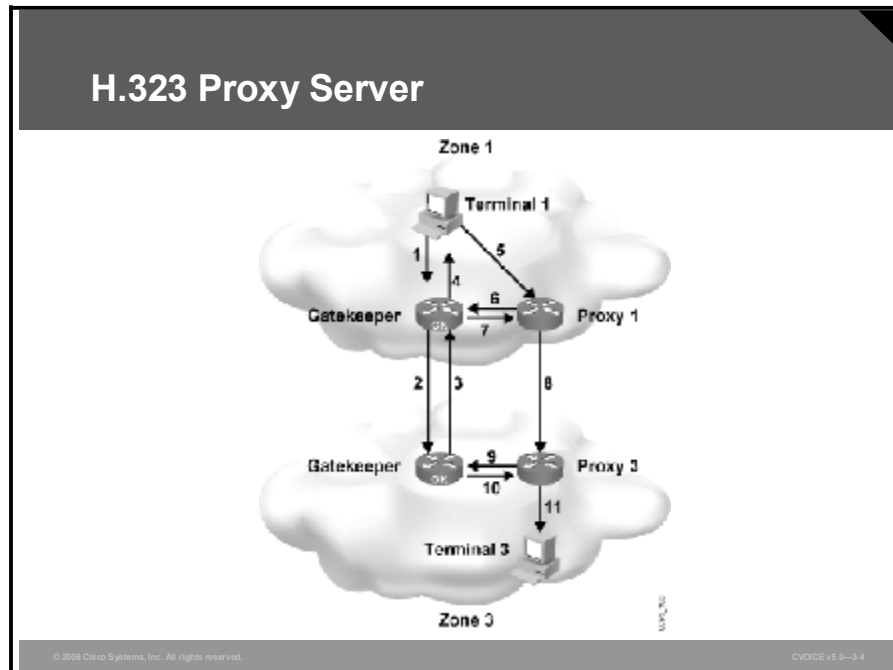
In H.323, the key components are the gateways and the gatekeeper. H.323 can employ any of these strategies:

- **Hot Standby Router Protocol (HSRP):** HSRP allows two gatekeepers to share both an IP address and access to a common LAN; however, at any time, only one gatekeeper is active. Endpoints are configured with the name of the gatekeeper, which they can resolve using the Domain Name System (DNS) or the IP address of the gatekeeper.
- **Virtual Router Redundancy Protocol (VRRP):** VRRP allows a group of gatekeepers on a multiaccess link to use the same virtual IP address, with one device acting as the master virtual router and one or more devices configured to be available as backup virtual routers. Endpoints are configured with the name or virtual IP address of the gatekeeper. VRRP is defined by the Internet Engineering Task Force (IETF) as RFC 3768.

- **Multiple gatekeepers with gatekeeper discovery:** Deployment of multiple gatekeepers reduces the probability of the total loss of gatekeeper access. However, adding new gatekeepers presents a new challenge. Each gatekeeper creates a unique H.323 zone. Because an H.323 endpoint is associated with only one gatekeeper at a time (in only one zone at a time), endpoints are configured to find only one of several working gatekeepers. Fortunately, a gateway can be configured with an ordered list of gatekeepers or to use IP multicast to locate a gatekeeper.
- **Multiple gatekeepers configured for the same prefix:** Gatekeepers send location request (LRQ) messages to other gatekeepers when locating an endpoint. By supporting the same prefix on multiple gatekeepers, the LRQ can be resolved by multiple gatekeepers. This strategy makes the loss of one gatekeeper less significant.
- **Multiple gateways configured for the same prefix:** Survivability is enhanced at the gateway with multiple gateways that are configured to reach the same switched circuit network (SCN) destination. By configuring the same prefix of destinations in multiple gateways, the gatekeeper sees the same prefix more than once as each gateway registers with its gatekeeper.

# H.323 Proxy Server

This topic describes a call setup scenario involving a proxy server.



An H.323 proxy server can circumvent the shortcomings of a direct path in cases where the direct path between two H.323 endpoints is not the most appropriate; for example, when the direct path has poor throughput and delay characteristics, when the direct path is not easily available because of a firewall, or when zones are configured as inaccessible on the gatekeepers to isolate addressing information in different zones.

When a proxy server is involved, two sessions are typically established as follows:

- Originating endpoint to the proxy server
- Proxy server to the terminating endpoint

However, when a proxy server also represents the terminating endpoint, a third session is required, as follows:

- Originating endpoint to proxy server 1
- Proxy server 1 to proxy server 2
- Proxy server 2 to terminating endpoint

## Example: H.323 Proxy

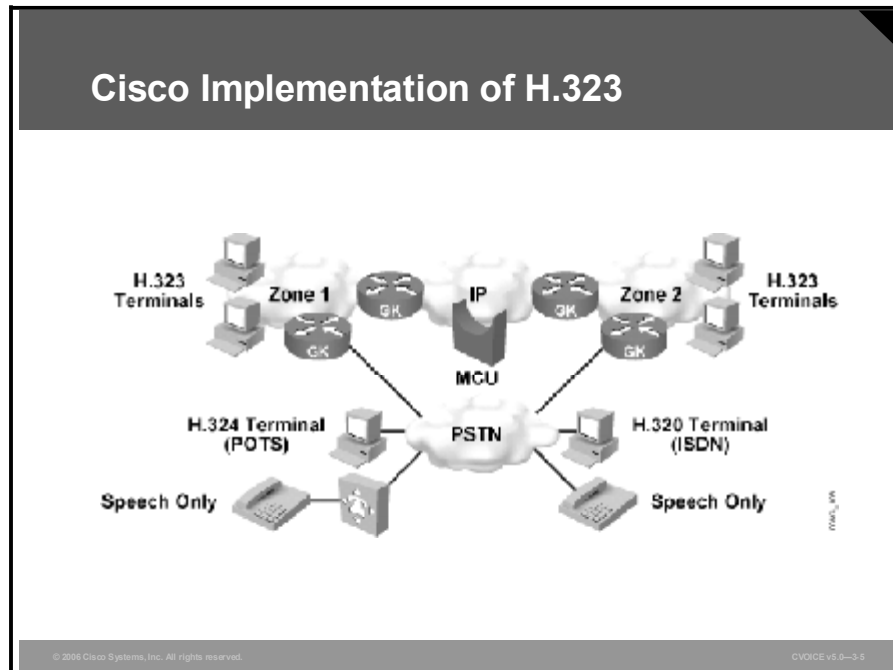
The figure illustrates an example with three sessions. The objective in this scenario is for terminal 1 and terminal 3 to establish an end-to-end relationship for multimedia communications. Here is the sequence of events that occurs:

1. Terminal 1 asks gatekeeper 1 for permission to call terminal 3.
2. Gatekeeper 1 locates gatekeeper 3 as the terminal 3 gatekeeper. Gatekeeper 1 asks gatekeeper 3 for the address of terminal 3.
3. Gatekeeper 3 responds with the address of proxy 3 (instead of the address of terminal 3) to hide the identity of terminal 3.
4. Gatekeeper 1 is configured to get to proxy 3 by way of proxy 1, so gatekeeper 1 returns the address of proxy 1 to terminal 1.
5. Terminal 1 calls proxy 1.
6. Proxy 1 consults gatekeeper 1 to discover the true destination of the call, which is terminal 3 in this example.
7. Gatekeeper 1 instructs proxy 1 to call proxy 3.
8. Proxy 1 calls proxy 3.
9. Proxy 3 consults gatekeeper 3 for the true destination, which is terminal 3.
10. Gatekeeper 3 gives the address of terminal 3 to proxy 3.
11. Proxy 3 completes the call to terminal 3.

Notice that the resulting path between terminal 1 and terminal 3 involves three separate legs: one between terminal 1 and proxy 1, one between proxy 1 and proxy 3, and one between proxy 3 and terminal 3. Both the media and any signaling are carried over these three legs.

# Cisco Implementation of H.323

This topic discusses how Cisco implements H.323.

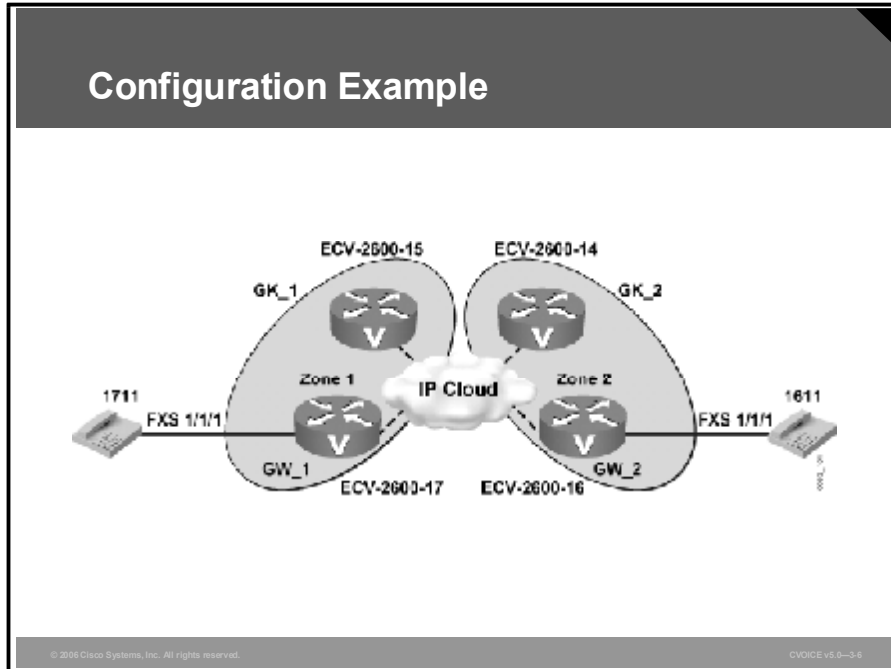


Cisco provides support for all H.323 components, including those listed here:

- **H.323 terminals:** Cisco provides support for H.323 terminals in Cisco IP Phones.
- **Gateways:** Cisco implements H.323 gateway support in these devices:
  - Cisco voice-enabled routers (first available in Cisco IOS Release 11.3)
  - Cisco SC2200 Signaling Controllers
  - Cisco PGW 2200 Public Switched Telephone Network (PSTN) Gateways
  - Voice-enabled Cisco AS5xx0 universal access servers
  - Cisco BTS 10200 Softswitch
- **Gatekeepers:** Cisco implements gatekeeper support in these products:
  - Cisco Multimedia Conference Manager
  - Cisco CallManager
  - Routers (first available in Cisco IOS Release 11.3)
- **Multipoint control unit (MCU):** The multipoint controller (MC) and multipoint processor (MP) of the Cisco IP/VC 3500 Series MCU support all H.323 conference types. The IP/VC 3500 Series MCU also incorporates a gatekeeper.
- **Other support:** Cisco PIX 500 Series firewalls and Context-Based Access Control (CBAC) support in the Cisco Secure Integrated Software monitor the logical channel handshaking of the H.245 control function and dynamically open conduits for the Real-Time Transport Protocol (RTP) sessions.

# Configuring H.323 Gateways

This topic illustrates and describes the configuration commands used to create a two-zone, two-gatekeeper scenario.



The figure illustrates the scenario on which the gateway configurations are based.



## Configuring the Gateways

### Gateway 1

```
hostrname ECV-2610-17
!
interface Ethernet0/0
 ip address 10.52.218.49 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id gk-somel.best.com ipaddr 10.52.218.47 1718
 h323-gateway voip h323-id gw 1
 h323-gateway voip bind srcaddr 10.52.218.49
!
dial-peer voice 1 voip
 destination-pattern 16..
 session target ras
!
dial-peer voice 2 pots
 destination-pattern 911
 port 1/1/1
 no register e164
!
Gateway
!
end
```

To use a gatekeeper, the user must complete these three tasks on the gateway:

1. Enable the gateway with the **gateway** command.
2. Configure the relationship with the gatekeeper. This requires these three interface subcommands:
  - **h323-gateway voip interface:** This command tells the router that this interface should be enabled for H.323 packet processing.
  - **h323-gateway voip id:** This command identifies the ID of the gatekeeper.
  - **h323-gateway voip h323-id:** This command configures the ID of this router. When the router registers with the gatekeeper, the gatekeeper recognizes the gateway by this ID.
3. Configure a dial peer to use the gatekeeper with the **ras** command on the dial peer command **session target**.

## Configuring the Gateways (Cont.)

### Gateway 2

```
hostname EGV-2610-16
!
interface Ethernet0/0
 ip address 10.52.218.48 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id gk-zone2.test.com ipaddr 10.52.218.46 1718
 h323-gateway voip h323-id gw 2
 h323-gateway voip bind srcaddr 10.52.218.40
!
dial-peer voice 1 voip
 destination-pattern 1/. .
 session target ras
!
dial-peer voice 2 pots
 destination-pattern 911
 port 1/1/1
 no register e164
!
Gateway
!
end
```

You can use other interface subcommands, one of which is illustrated in the configuration for both gateways. The command in the figure performs these functions:

- **h323-gateway voip tech-prefix 1#**: Registers a technology prefix
- **h323-gateway voip bind srcaddr 10.52.218.48**: Sets the source address in H.323 packets

A technology prefix advises the gatekeeper that this gateway can handle type 1# destinations. For routing purposes, a technology prefix may be assigned to a multimedia type, such as video. By registering type 1# support, the gateway supports the video applications.

In the dial peer, the **no register e164** subcommand causes the gateway not to register the destination pattern when communicating with the gatekeeper. When the dial peer does not register its prefix, the dial peer requires an alternative mechanism for the gatekeeper to acquire this information.

# Configuring H.323 Gatekeepers

This topic illustrates the gatekeeper configuration for a two-zone, two-gatekeeper scenario.

## Configuring the Gatekeepers

### Gatekeeper 1

```
hostname ECV-2610-15
!
interface Ethernet0/0
 ip address 10.52.218.47 255.255.255.0
!
Gatekeeper
 zone local gk-zone1.test.com test.com 10.52.218.47
 zone remote gk-zone2.test.com test.com 10.52.218.46 1719
 zone prefix gk-zone2.test.com 16..
 zone prefix gk-zone1.test.com 17..
 gw-type-prefix 1#* default-technology
 no shutdown
!
end
```

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-9

The gatekeeper application is enabled with the **gatekeeper** command.

For this example, the gateways are configured to withhold their E.164 addresses, so the gatekeepers must define the addresses locally. This is done with the **zone prefix** command. In the example, each gatekeeper has two **zone prefix** commands, the first pointing to the other gatekeeper and the second pointing to the local zone (meaning the prefix is in the local zone). The **zone prefix** command that points to itself is configured with the name of the gateway used to direct traffic to the destination. The address of the gateway is not required, because it is determined automatically when the gateway registers. The commands in the figure perform these functions:

- **zone local gk-zone1.test.com test.com 10.52.218.47:** Defines the ID of the local gatekeeper
- **zone remote gk-zone2.test.com test.com 10.52.218.46 1719:** Defines the identity and IP address of neighboring gatekeepers

## Configuring the Gatekeepers (Cont.)

### Gatekeeper 2

```
hostname ECV-2610-14
!
interface Ethernet0/0
 ip address 10.52.218.46 255.255.255.0
!
Gatekeeper
 zone local gk-zone2.test.com test.com 10.52.218.46
 zone remote gk-zone1.test.com test.com 10.52.218.47 1719
 zone prefix gk-zone2.test.com 16..
 zone prefix gk-zone1.test.com 17..
 gw-type-prefix 1#* default-technology
 no shutdown
!
end
```

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-3-10

Because the gateways register their technology prefixes, the gatekeeper does not need to be configured. If a technology prefix is required, the **gw-type-prefix** command defines a technology prefix, and can manually update technology prefix knowledge in the gatekeeper. In the example configuration in this figure, the gatekeeper attempts to define a technology prefix as the default with the command **gw-type-prefix 1#\* default-technology**. Any unknown destination is assumed to be of the default technology type, and calls are forwarded to any gateway that registered the default technology type.

# Monitoring and Troubleshooting

The **show** and **debug** commands are valuable when examining the status of the H.323 components and during troubleshooting. This topic lists many **show** and **debug** commands that are used to provide support for monitoring and troubleshooting H.323.

## Example: show Command

```
Router# show gatekeeper calls
Total number of active calls = 1.
GATEKEEPER CALL INFO

LocalCallID Age(sec) BW
12-3339 94 768 (Kbps)
 Endpt(s):Alias E.164Addr CallSignalAddr Port
RFSignalAddr Port
src EP:epA 90.0.0.11 1720
90.0.0.11 1700
dst EP:egBzoneB.com
src FX:pxA 90.0.0.01 1720
90.0.0.01 24999
dst FX:pxB 172.21.139.90 1720
172.21.139.90 24999
```

Here are some of the **show** commands used for H.323:

- **show call active voice [brief]:** Displays the status, statistics, and parameters for all active voice calls
- **show call history voice [last n|record|brief]:** Displays call records from the history buffer
- **show gateway:** Displays the current status of the H.323 gateway configured in the router
- **show gatekeeper calls:** Displays the active calls for which the gatekeeper is responsible (illustrated in the figure)
- **show gatekeeper endpoints:** Displays status of all registered endpoints for a gatekeeper
- **show gatekeeper gw-type-prefix:** Displays the current technology prefix table
- **show gatekeeper status:** Displays the current status of the gatekeeper
- **show gatekeeper zone prefix:** Displays the gateways and their associated E.164 prefixes
- **show gatekeeper zone status:** Displays the status of the connections to gateways in the local zone and the status of the connections to gatekeepers in other zones

## Selected debug Commands

Here are some of the **debug** commands used for H.323:

- **debug voip ccapi inout:** This command shows every interaction with the call control application programming interface (API) on the telephone interface and the VoIP side. Monitoring the **debug voip ccapi inout** command output allows users to follow the progress of a call from the inbound interface or VoIP peer to the outbound side of the call. Because this **debug** command is highly active, use it sparingly in a live network.
- **debug cch323 h225:** This command traces the transitions in the H.225.0 state machine during the establishment of the call control channel. The first step in establishing a relationship between any two components is to bring up the call control channel. Monitoring the output of the **debug cch323 h225** command allows users to follow the progress and determine if the channel is established correctly.
- **debug cch323 h245:** This command traces the state transitions in the H.245 state machine during the establishment of the H.245 control channel. Monitoring the output of the **debug cch323 h245** command allows users to follow the progress to see if the channel is established correctly.
- **debug cch323 ras:** This command traces the state transition in the establishment of the registration, admission, and status (RAS) control channel. Monitoring the output of the **debug cch323 ras** command allows users to determine if the channel is established correctly.
- **debug h225 asn1:** This command displays an expansion of the Abstract Syntax Notation One (ASN.1)-encoded H.225.0 messages. When investigating VoIP peer association problems, this **debug** command helps users monitor the activity of the call-signaling channel. Because H.225.0 encapsulates H.245, this is a useful approach for monitoring both H.225.0 and H.245.
- **debug h225 events:** This command is similar to the ASN.1 version of the command but does not expand the ASN.1. Debugging events usually imposes a lighter load on the router.
- **debug h245 asn1:** This command is similar to the H.225.0 variant except that it displays only the H.245 messages.
- **debug h245 events:** This command is similar to the H.225.0 variant except that it displays only the H.245 messages.

# Summary

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

## Summary

- **H.323 uses HSRP and multiple gateways and gatekeepers to mitigate failures.**
- **An H.323 proxy server can be placed between components to enhance security or to take advantage of routing features.**
- **Cisco provides support for all H.323 components, including terminals, gateways, gatekeepers, and MCUs.**
- **To configure a gateway, you must enable the gateway, configure the relationship with the gatekeeper, and configure a dial peer to use the gatekeeper.**
- **To configure a gatekeeper, you must enable the gatekeeper, define the ID of the local gatekeeper and the ID and IP address of neighboring gatekeepers, and if necessary, define technology prefixes and zone prefixes.**
- **Several show and debug commands can be used to monitor and troubleshoot H.323.**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE vs.0-3-10

## References

For additional information, refer to these resources:

- ITU-T Recommendation H.323 (version 4).  
<http://www.itu.int/rec/recommendation.asp?type=items&lang=E&parent=T-REC-H.323-200011-S>.
- *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).
- *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2*.  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_command\\_reference\\_book09186a0080080c8b.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080080c8b.html).

## Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 3-1: Configuring VoIP with H.323

# 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) In H.323, which survivability strategy allows two gatekeepers to share an IP address?
- A) HSRP or VRRP
  - B) multiple gateways configured for the same prefix
  - C) multiple gatekeepers configured for the same prefix
  - D) multiple gatekeepers with gatekeeper discovery
- Q2) What is the problem with having multiple gatekeepers in a network?
- A) Only one of the gatekeepers can be active at any given time.
  - B) Endpoints are configured to find only one of several working gatekeepers in the network.
  - C) Network components are hard to configure.
  - D) The H.323 zones may overlap.
- Q3) What is the role of an H.323 proxy server?
- A) provides an alternate path when the direct path is not the most appropriate
  - B) performs MC services for a multipoint conference
  - C) substitutes for a gatekeeper if that gatekeeper goes down
  - D) provides the control channel for audio and video data streams
- Q4) When H.323 proxy servers are being used on a network, which situation would require three sessions to set up a call?
- A) when authentication is required
  - B) when the direct path has poor throughput
  - C) when the proxy server also represents the terminating endpoint
  - D) when zones are configured as inaccessible on the gatekeeper
- Q5) Which Cisco application supports H.323 gatekeepers?
- A) Cisco IP Phone
  - B) Cisco CallManager
  - C) Cisco Secure Integrated Software
  - D) Cisco voice-enabled switches
- Q6) Which H.323 component is supported by Cisco SC2200 Signaling Controllers?
- A) terminals
  - B) gateways
  - C) gatekeepers
  - D) MCU
- Q7) What is the function of the **session target ras** subcommand in H.323 gateway configuration?
- A) configures a dial peer to use the gatekeeper
  - B) identifies the ID of the gatekeeper
  - C) registers the destination gatekeeper
  - D) configures the remote gatekeeper



- Q8) When you are configuring an H.323 gateway, which three tasks do you need to do to configure the relationship with the gatekeeper? (Choose three.)
- A) enable the gateway
  - B) tell the router which interface should be enabled for H.323 packet processing
  - C) configure a dial peer to use the gateway
  - D) identify the gatekeeper ID
  - E) configure the gateway ID
  - F) tell the gateway not to register the destination pattern
- Q9) Which command tells the gatekeepers to define addresses locally?
- A) **zone prefix**
  - B) **zone local**
  - C) **zone remote**
  - D) **zone default**
- Q10) This command is configured on a gatekeeper:
- ```
zone remote gk-zone2.test.com test.com 10.52.218.46 1719
```
- What is the function of this command?
- A) defines a technology prefix
 - B) defines the identity and IP address of neighboring gatekeepers
 - C) defines the identity and IP address of the local gatekeeper
 - D) defines the IP address of the gateway to which default calls will be forwarded
- Q11) Which **show** command is used to display the status of all registered endpoints for a gatekeeper?
- A) **show gatekeeper gw-type-prefix**
 - B) **show gatekeeper zone prefix**
 - C) **show gatekeeper endpoints**
 - D) **show gatekeeper status**
- Q12) Which **debug** command should you use to monitor the activity of the H.225.0 and H.245 call-signaling channels on a busy network?
- A) **debug h225 asn1**
 - B) **debug h225 events**
 - C) **debug h245 asn1**
 - D) **debug h245 events**

Lesson Self-Check Answer Key

- Q1) A
Relates to: Robust Design
- Q2) B
Relates to: Robust Design
- Q3) A
Relates to: H.323 Proxy Server
- Q4) C
Relates to: H.323 Proxy Server
- Q5) B
Relates to: Cisco Implementation of H.323
- Q6) B
Relates to: Cisco Implementation of H.323
- Q7) A
Relates to: Configuring H.323 Gateways
- Q8) B, D, E
Relates to: Configuring H.323 Gateways
- Q9) A
Relates to: Configuring H.323 Gatekeepers
- Q10) B
Relates to: Configuring H.323 Gatekeepers
- Q11) C
Relates to: Monitoring and Troubleshooting
- Q12) A
Relates to: Monitoring and Troubleshooting

Lesson 4

Configuring SIP

Overview

This lesson describes how to configure the session initiation protocol (SIP) and explores the features and functions of the SIP environment, including its components, how these components interact, and how to accommodate scalability and survivability.

Relevance

An understanding of the features and functions of SIP components, and the relationships that the components establish with each other, is important in implementing a scalable, resilient, and secure SIP environment.

Objectives

Upon completing this lesson, you will be able to configure, monitor, and troubleshoot SIP on a Cisco router. This ability includes being able to meet these objectives:

- Describe three IETF standards that help SIP in the establishment, maintenance, and termination of multimedia sessions
- List the types of user agents and servers that are used by SIP and describe their functions
- List six examples of SIP request and response messages
- Identify three types of SIP addresses and the servers that are involved in address registration and resolution
- Describe three SIP call setup procedures and list their advantages and disadvantages
- Illustrate two strategies that are used by SIP to provide fault tolerance
- List SIP gateway and network server devices that are supported by Cisco
- Use the **sip-ua** command with subcommands to configure SIP on a Cisco router
- Use **show** and **debug** commands to monitor and troubleshoot SIP

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- An understanding of the objectives and principles of signaling and call control in the context of VoIP

Outline

The outline lists the topics included in this lesson.

Outline

- Overview
- Session Initiation Protocol
- Components of SIP
- SIP Messages
- SIP Addressing
- Call Setup Models
- Robust Design
- Cisco Implementation of SIP
- Configuring SIP on a Cisco Router
- Monitoring and Troubleshooting
- Summary
- Lesson Self-Check

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-2

Session Initiation Protocol

SIP provides another framework for establishing and maintaining Voice over IP (VoIP) calls. This topic describes SIP and its standards.

SIP and Associated Standards

- **SIP is a simple extensible protocol.**
- **SIP is defined in IETF RFC 2543; RFC 3261.**
- **SIP creates, modifies, and terminates multimedia sessions with one or more participants.**
- **SIP leverages various IETF standards: RTP, Real-Time Transport Control Protocol (RTCP), HTTP, SDP, DNS, SAP, and Real Time Streaming Protocol (RTSP).**
- **SIP performs addressing by E.164, e-mail, or DNS service record.**
- **SIP is ASCII text-based for easy implementation and debugging.**

SIP is a signaling and control protocol for the establishment, maintenance, and termination of multimedia sessions with one or more participants. SIP multimedia sessions include Internet telephone calls, multimedia conferences, and multimedia distribution. Session communications may be based on multicast, unicast, or both.

SIP operates on the principle of session invitations. Through invitations, SIP initiates sessions or invites participants into established sessions. Descriptions of these sessions are advertised by any one of several means, including the Session Announcement Protocol (SAP) defined in RFC 2974, which incorporates a session description according to the Session Description Protocol (SDP) defined in RFC 2327.

SIP uses other Internet Engineering Task Force (IETF) protocols to define other aspects of VoIP and multimedia sessions; for example, URLs for addressing, Domain Name System (DNS) for service location, and Telephony Routing over IP (TRIP) for call routing.

SIP supports personal mobility and other Intelligent Network (IN) telephony subscriber services through name mapping and redirection services. Personal mobility allows a potential participant in a session to be identified by a unique personal number or name.

IN provides carriers with the ability to rapidly deploy new user services on platforms that are external to the switching fabric. Access to the external platforms is by way of an independent vendor and standard user interface. Calling-card services, toll-free number services, and local number portability are just three of these services.

Multimedia sessions are established and terminated by these services:

- **User location services:** Locate an end system
- **User capabilities services:** Select the media type and parameters
- **User availability services:** Determine the availability and desire for a party to participate
- **Call setup services:** Establish a session relationship between parties and manage call progress
- **Call handling services:** Transfer and terminate calls

Although the IETF has made great progress in defining extensions that allow SIP to work with legacy voice networks, the primary motivation behind the protocol is to create an environment that supports next-generation communication models that use the Internet and Internet applications.

SIP is described in IETF RFC 3261 (June 2002), which renders obsolete RFC 2543 (March 1999).

Example: Cisco SIP Support

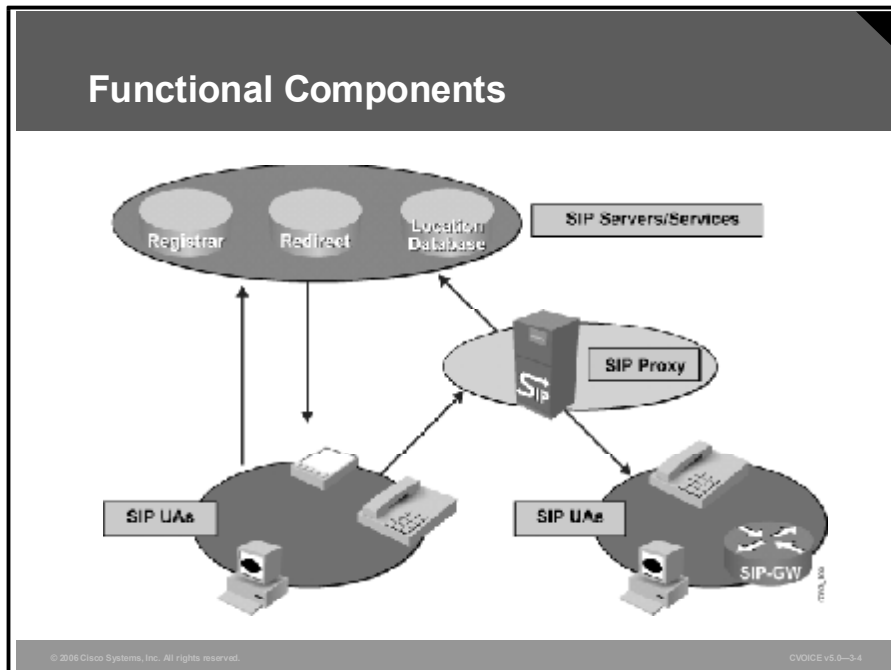
The Cisco SIP-enabled product portfolio encompasses all components of a SIP network infrastructure, from IP Phones and access devices to call control and public switched telephone network (PSTN) interworking. The first Cisco SIP products were deployed with live traffic several years ago. All of the products listed here are deployed in live networks spanning a variety of applications and continents:

- **Cisco IP Phones:** The Cisco IP Phone series, including the Cisco IP Phone 7970, Cisco IP Phone 7960 and Cisco IP Phone 7940, support SIP user agent (UA) functionality. These IP Phones deliver functionality such as inline power support and dual Ethernet ports, and deliver traditional desktop functionality such as call hold, transfer, conferencing, caller ID, call waiting, and a lighted message waiting indicator.
- **Cisco Analog Telephone Adaptor (Cisco ATA 186):** The Cisco ATA 186 supports SIP UA functionality. With two Foreign Exchange Station (FXS) ports and a single Ethernet port, the ATA 186 provides a low-cost means to connect analog phones to a SIP network. The ATA 186 also delivers traditional desktop functionality such as call hold, transfer, conferencing, caller ID, and lighted call-waiting and message waiting indicators.
- **Cisco packet voice gateways:** The Cisco Series 1700 Modular Access Routers that are voice-capable, Cisco 2600 Series multiservice platforms, Cisco 3800 Series Integrated Services Routers, 3700 Series Integrated Services Routers, Cisco AS5000 Series Universal Gateways, and Cisco 7200 Series voice gateways all support SIP UA functionality. These products provide a means of connecting SIP networks to traditional time-division multiplexing (TDM) networks via T1, E1, digital service level 3 (DS3), channel associated signaling (CAS), PRI or BRI, R2 signaling, FXS, Foreign Exchange Office (FXO), or ear and mouth (E&M) interfaces. Cisco packet voice gateways are used to build the largest packet telephony networks in the world.

- **Cisco SIP Proxy Server:** The Cisco SIP Proxy Server provides the functionality of a SIP proxy, SIP redirect, SIP registrar, and SIP location services server. The Cisco SIP Proxy Server provides the foundation for call routing within SIP networks; it can interwork with traditional SIP location services such as DNS or telephone number mapping (E.164 number [ENUM]), with feature servers via a SIP redirect message, and with H.323 location services using standard location request (LRQ) messages. The Cisco SIP Proxy Server runs on either Solaris or Linux operating systems.
- **Cisco BTS 10200 Softswitch:** The Cisco BTS 10200 Softswitch provides softswitch functionality to Class 4 and Class 5 networks, and provides SIP-to-Signaling System 7 (SS7) gateway functionality for American National Standards Institute (ANSI) standardized networks. The BTS 10200 Softswitch supports SIP UA functionality in conjunction with a Cisco packet voice media gateway, such as a Cisco AS5000 Series Universal Gateway or a Cisco MGX 8000 Series Voice Gateway.
- **Cisco PGW 2200 PSTN Gateway:** The Cisco PGW 2200 PSTN Gateway provides softswitch functionality for Class 4 networks, as well as Internet offload and SIP-to-SS7 gateway functionality for international networks. The PGW 2200 PSTN Gateway supports ISDN User Part (ISUP) certification in over 130 countries. The PGW 2200 PSTN Gateway supports SIP UA functionality in conjunction with a Cisco packet voice media gateway such as an AS5000 Series Universal Gateway or MGX 8000 Series Voice Gateway.
- **Cisco PIX Security Appliance and Cisco Adaptive Security Appliance (ASA):** The Cisco PIX Security Appliance and the Cisco ASA are SIP-aware networking devices that provide firewall and Network Address Translation (NAT) functionality. Because these devices are SIP-aware, they are able to dynamically allow SIP signaling to traverse network and addressing boundaries without compromising overall network security. The Cisco PIX Security Appliance and the Cisco ASA functioning in this capacity are called application layer gateways (ALGs).

Components of SIP

SIP is modeled on the interworking of UAs and network servers. This topic describes the functional and physical components of a UA.



SIP is a peer-to-peer protocol. The peers in a session are called UAs. A UA consists of these 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 UA can function as a UAC *or* a UAS during a session, but not both in the same session. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request; the initiating UA uses a UAC and the terminating UA uses a UAS.

From an architectural standpoint, the physical components of a SIP network are grouped into these two categories:

- **UAs:** SIP UAs include these devices:
 - **IP telephone:** An IP telephone 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:** A gateway acts as a UAS or UAC and provides call control support. Gateways provide many services, the most common being a translation function between SIP UAs 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 these types:
 - **Proxy server:** A proxy server is 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:** A redirect server provides a UA with information about the next server that the UA should contact. The server can be another network server or a UA. The UA redirects the invitation to the server identified by the redirect server.
 - **Registrar server:** A registrar server makes requests from UACs for registration of their current location. Registrar servers are often located near or even colocated with other network servers, most often a location server.
 - **Location server:** A location server is 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 protocol, Referral Whois (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 voice register mode request communication between SIP components and a location server is not standardized.

Example: SIP Applications

Leaders in the communications industry are developing new products and services that rely on SIP, and they are offering attractive new communications services to their customers. Microsoft recently added support for SIP clients in core product offerings—Microsoft Windows XP and Microsoft Windows Messenger—a step that will proliferate SIP clients on personal computers worldwide. SIP is gaining momentum in every market.

Cisco is enabling the advance of new communications services with a complete SIP-enabled portfolio, including proxy servers, packet voice gateways, call control and signaling, IP Phones, and firewalls. Cisco solutions support a variety of call control and standard protocols, including H.323, Media Gateway Control Protocol (MGCP), and SIP, which can coexist in the same customer network.

SIP Messages

Communication between SIP components uses a request and response message model. This topic describes the types, use, and structure of these messages.

SIP Messages

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP
pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-3-5

SIP communication involves these two messages:

- **Request from a client to a server:** Consists of a request line, header lines, and a message body
- **Response from a server to a client:** Consists of a status line, header lines, and a message body

All SIP messages are text-based and modeled on RFC 822, *Standard for the Format of ARPA Internet Text Messages*, and RFC 2068, *Hypertext Transfer Protocol—HTTP/1.1*.

SIP defines four types of headers: a general header, an entity header, a request header, and a response header. The first two types of headers appear on both message types. The latter two types of headers are specific to request and response, respectively.

SIP Request Messages

- **INVITE:** Indicates that a user or service is being invited to participate in a call session
- **ACK:** Confirms that a client has received a final response to an INVITE request
- **BYE:** Terminates an existing call; can be sent by either UA
- **CANCEL:** Cancels pending searches; does not terminate calls that have been accepted
- **OPTIONS:** Queries the capabilities of servers
- **REGISTER:** Registers the UA with the registrar server of a domain

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-3-6

In the request line, SIP uses a message to indicate the action to be taken by the responding component (usually a server).

These request messages indicate the action that the responding component should take:

- **INVITE:** A client originates the INVITE message to indicate that the server is invited to participate in a session. An invitation includes a description of the session parameters.
- **Acknowledgment (ACK):** A client originates the ACK message to indicate that the client has received a response to its earlier invitation.
- **BYE:** A client or server originates the BYE message to initiate call termination.
- **CANCEL:** A client or server originates the CANCEL message to interrupt any request currently in progress. CANCEL is *not* used to terminate active sessions.
- **OPTIONS:** A client uses the OPTIONS message to solicit capabilities information from a server. This method is used to confirm cached information about a UA or to check the ability of a UA to message accept an incoming call.
- **REGISTER:** A UA uses the REGISTER message to provide information to a network server. Registrations have a finite life and must be renewed periodically. This prevents the use of stale information when a UA moves.

SIP Response Messages

- **1xx: Informational response**
- **2xx: Successful response**
- **3xx: Redirection response**
- **4xx: Client error response**
- **5xx: Server error response**
- **6xx: Global failure response**

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-3.7

SIP response messages are sent in response to a request and indicate the outcome of request interpretation and execution. Responses take one of three basic positions: success, failure, or provisional. A status code reflects the outcome of the request.

Status Codes

These response messages indicate the status of a request:

- **1xx (informational):** Provisional response; indicates that the request is still being processed
- **2xx (successful):** Indicates that the requested action is complete and successful
- **3xx (redirection):** Indicates that the requestor requires further action (for example, a redirect server responds with “moved” to advise the client to redirect its invitation)
- **4xx (client error):** Fatal response; indicates that the client request is flawed or impossible to complete
- **5xx (server error):** Fatal response; indicates that the request is valid but the server failed to complete it
- **6xx (global failure):** Fatal response. Indicates that the request cannot be fulfilled by any server.

SIP Addressing

To obtain the IP address of a SIP UAS or a network server, a UAC performs address resolution of a user identifier. This topic describes address formats, address registration, and address resolution.

Addresses

- **Fully qualified domain names**
 - `sip:jdoe@cisco.com`
- **E.164 addresses**
 - `sip:14085551234@gateway.com; user=phone`
- **Mixed addresses**
 - `sip:14085551234; password=changeme@10.1.1.1`
 - `sip:jdoe@10.1.1.1`

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v9.0-3.8

An address in SIP is defined in the syntax for a URL with “sip:” or “sips:” (for secure SIP connections) as the URL type. SIP URLs are used in SIP messages to identify the originator, the current destination, the final recipient, and any contact party. When two UAs communicate directly with each other, the current destination and final recipient URLs are the same. However, the current destination and the final recipient are different if a proxy or redirect server is used.

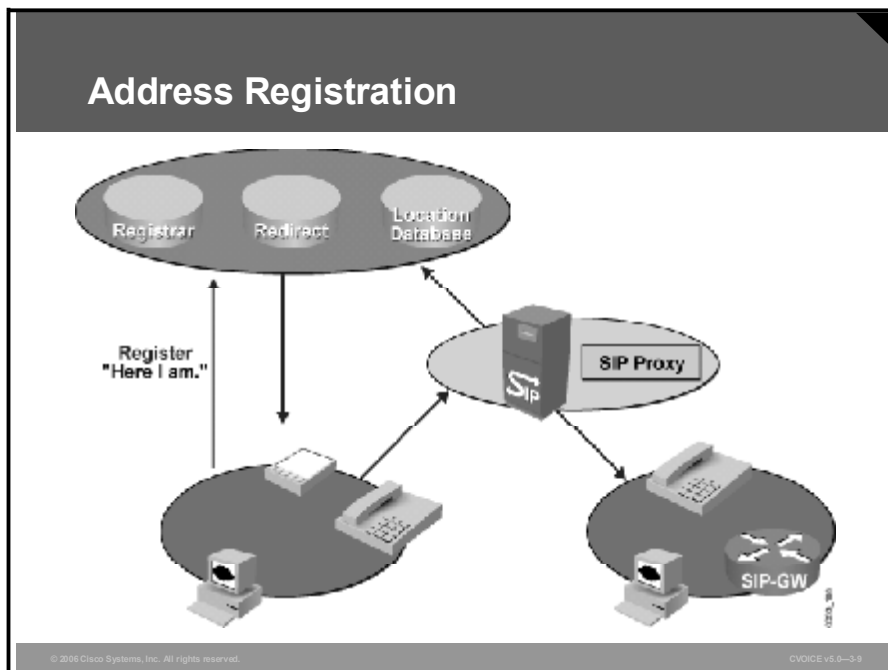
An address consists of an optional user ID, a host description, and optional parameters to qualify the address more precisely. The host description may be a domain name or an IP address. A password is associated with the user ID, and a port number is associated with the host description.

Example: SIP Addressing Variants

The figure provides examples of SIP addresses.

In the example “`sip:14085551234@gateway.com; user=phone`”, the “`user=phone`” parameter is required to indicate that the user part of the address is a telephone number. Without the “`user=phone`” parameter, the user ID is taken literally as a numeric string. The “`1408559876`” in the URL “`sip:1408559876@10.1.1.1`” is an example of a numeric user ID. In the same example, the password “`changeme`” is defined for the user.

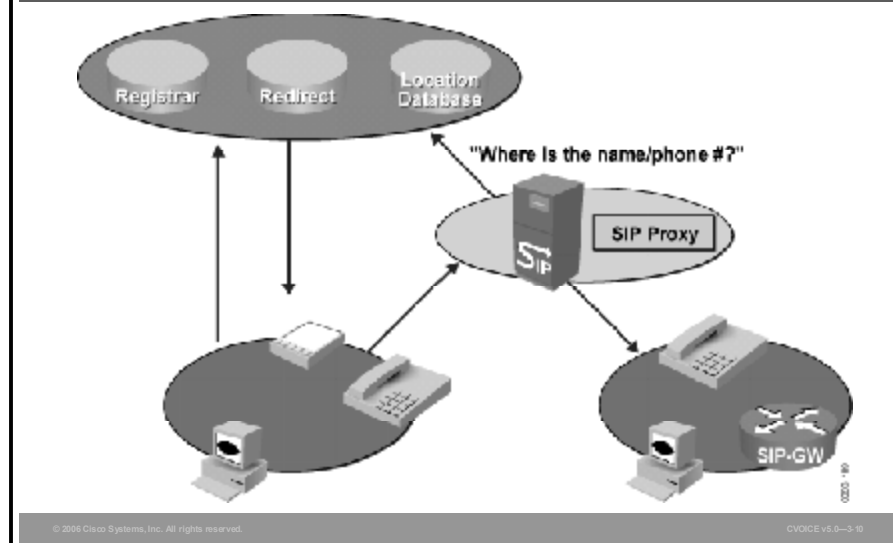
Address Registration



A SIP address is acquired in several ways: by interacting with a user, by caching information from an earlier session, or by interacting with a network server. For a network server to assist, it must recognize the endpoints in the network. This knowledge is abstracted to reside in a location server and is dynamically acquired by its registrar server.

To contribute to this dynamic knowledge, an endpoint registers its user addresses with a registrar server. The figure illustrates a voice REGISTER mode request to a registrar server.

Address Resolution

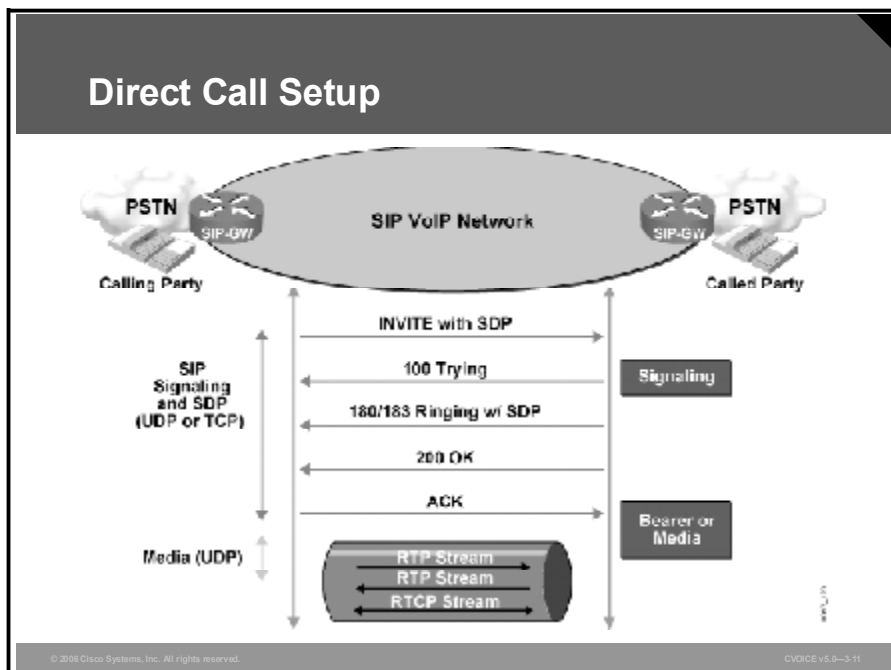


To resolve an address, a UA uses a variety of internal mechanisms such as a local host table, DNS lookup, Finger protocol, rwhois, or LDAP, or it leaves that responsibility to a network server. A network server uses any of the tools available to a UA or interacts through a nonstandard interface with a location server.

The figure illustrates a SIP proxy server resolving the address by using the services of a location server.

Call Setup Models

If a UAC recognizes the destination UAS, the client communicates directly with the server. In situations in which the client is unable to establish a direct relationship, the client solicits the assistance of a network server. This topic illustrates three interworking models for call setup: direct, using a proxy server, and using a redirect server.



When a UA recognizes the address of a terminating endpoint from cached information, or has the capacity to resolve it by some internal mechanism, the UAC may initiate direct (UAC-to-UAS) call setup procedures.

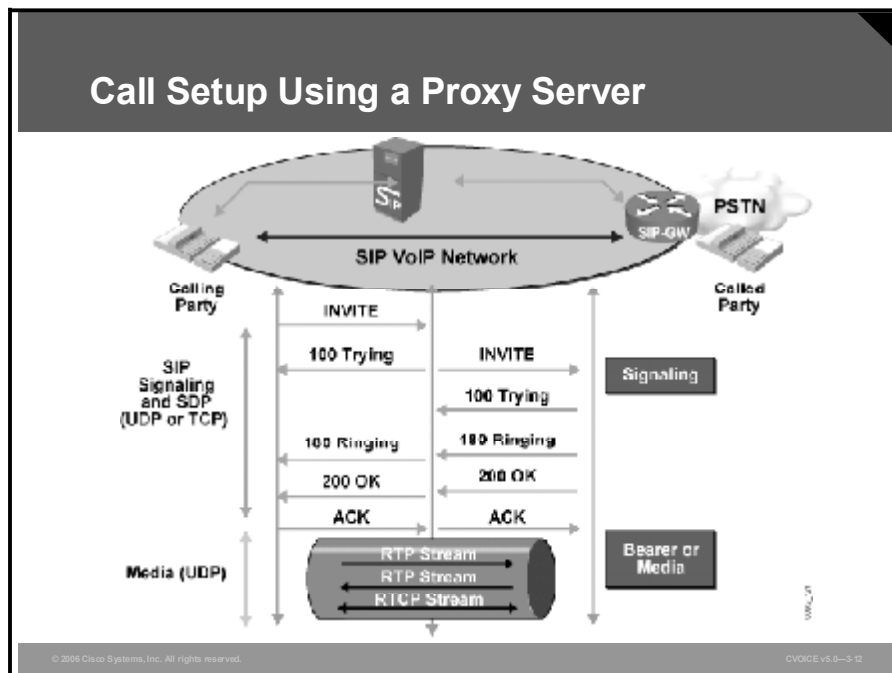
Direct setup is the fastest and most efficient of the call setup procedures. However, direct setup has some disadvantages. It relies on cached information or internal mechanisms to resolve addresses, which can become outdated if the destination is mobile. In addition, if the UA must keep information on a large number of destinations, management of the data can become prohibitive. This makes the direct method non-scalable.

Direct call setup proceeds as follows:

1. The originating UAC sends an invitation (INVITE) to the UAS of the recipient. The message includes an endpoint description of the UAC and SDP.
2. If the UAS of the recipient determines that the call parameters are acceptable, it responds positively to the originator UAC.
3. The originating UAC issues an ACK.

At this point, the UAC and UAS have all the information that is required to establish Real-Time Transport Protocol (RTP) sessions between them.

Call Setup Using a Proxy Server



The proxy server procedure is transparent to a UA. The proxy server intercepts and forwards an invitation to the destination UA on behalf of the originator.

A proxy server responds to the issues of the direct method by centralizing control and management of call setup and providing a more dynamic and up-to-date address resolution capability. The benefit to the UA is that it does not need to learn the coordinates of the destination UA, yet can still communicate with the destination UA. The disadvantages of this method are that using a proxy server requires more messaging and creates a dependency on the proxy server. If the proxy server fails, the UA is incapable of establishing its own sessions.

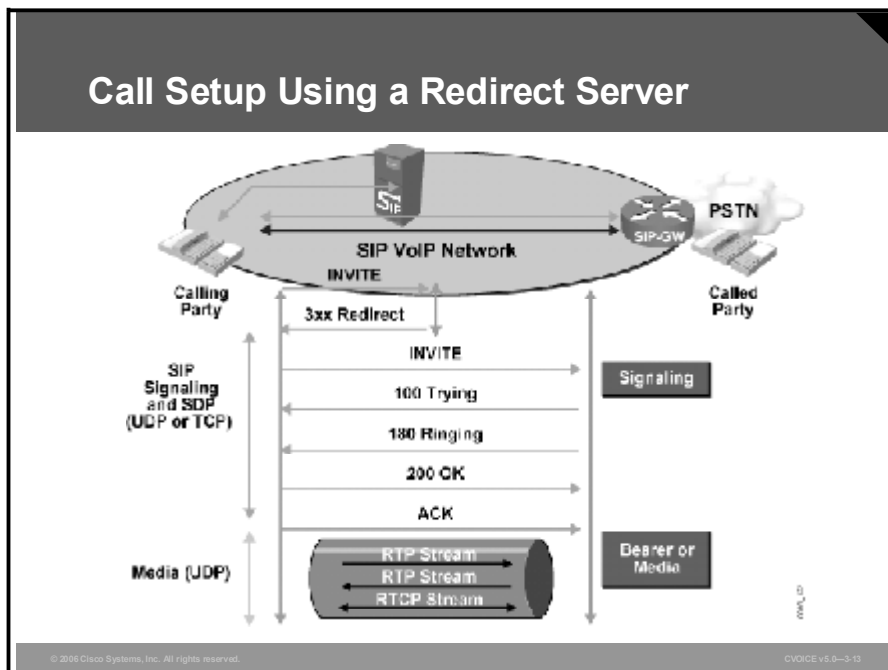
Note Although the proxy server acts on behalf of a UA for call setup, the UAs establish RTP sessions directly with each other.

When a proxy server is used, the call setup procedure is as follows:

1. The originating UAC sends an invitation (INVITE) to the proxy server.
2. The proxy server, if required, consults the location server to determine the path to the recipient and its IP address.
3. The proxy server sends the INVITE to the UAS of the recipient.
4. If the UAS of the recipient determines that the call parameters are acceptable, it responds positively to the proxy server.
5. The proxy server responds to the originating UAC.
6. The originating UAC issues an ACK.
7. The proxy server forwards the ACK to the recipient UAS.

The UAC and UAS now have all the information required to establish RTP sessions.

Call Setup Using a Redirect Server



A redirect server is programmed to discover a path to the destination. Instead of forwarding the INVITE to the destination, the redirect server reports back to a UA with the destination coordinates that the UA should try next.

A redirect server offers many of the advantages of the proxy server. However, the number of messages involved in redirection is fewer than with the proxy server procedure. The UA has a heavier workload because it must initiate the subsequent invitation.

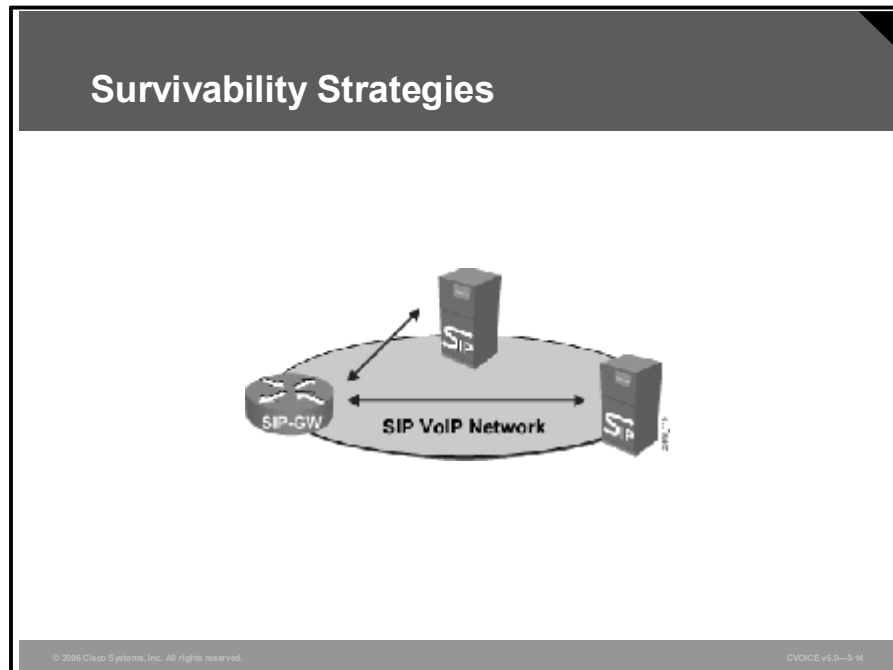
When a redirect server is used, the call setup procedure is as follows:

1. The originating UAC sends an invitation (INVITE) to the redirect server.
2. The redirect server, if required, consults the location server to determine the path to the recipient and its IP address.
3. The redirect server returns a “moved” response to the originating UAC with the IP address obtained from the location server.
4. The originating UAC acknowledges the redirection.
5. The originating UAC sends an INVITE to the remote UAS.
6. If the UAS of the recipient determines that the call parameters are acceptable, it responds positively to the UAC.
7. The originating UAC issues an ACK

The UAC and UAS now have all the information that is required to establish RTP sessions between them.

Robust Design

Maintaining high availability of a SIP environment requires a design that accommodates the failure of a network server. This topic describes strategies for maintaining VoIP service.



In a SIP environment, the failure of a network server cripples UAs that are dependent on that server. In SIP, the network servers are the proxy server, the redirect server, and the location server.

The most obvious way to preserve access to the critical components is to implement multiple instances of access.

For replication of a proxy or redirect server to be effective, a UA must have the ability to locate an active server dynamically. You can achieve this in any of these ways:

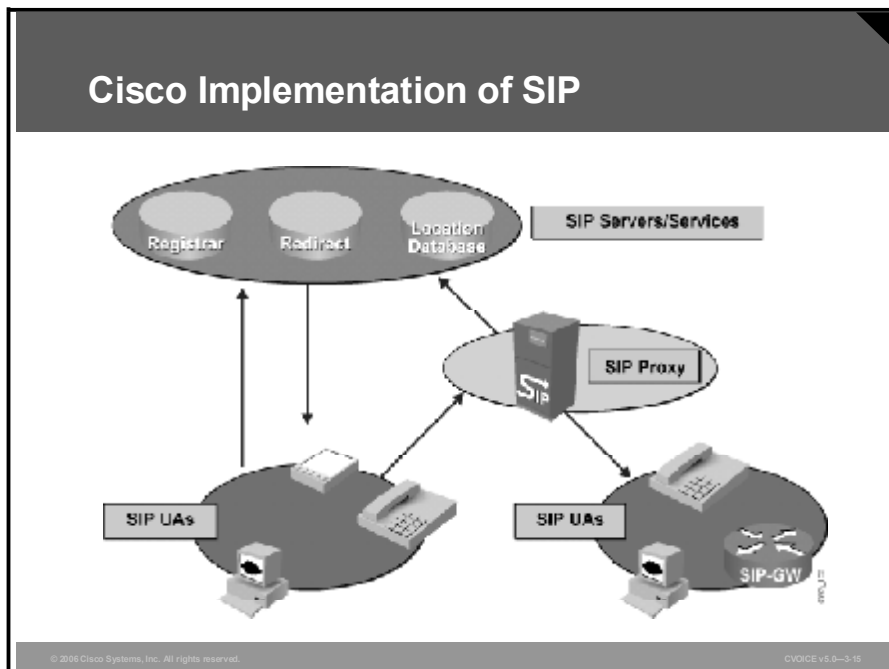
- Preconfigure a UA with the address of at least two of the servers. If access to its first choice fails, it shifts to the second.
- If all servers are configured with the same name, you must configure a UA to look up the name using DNS. The DNS query returns the addresses of all the servers matching the name, and the UA proceeds down the list until it finds one that works.

Example: SIP Survivability

The figure illustrates replication of SIP servers for survivability.

Cisco Implementation of SIP

This topic describes how Cisco implements SIP.



Cisco provides support for these SIP components:

- **SIP UAs:** Cisco provides support for SIP UA in Cisco IP Phone.

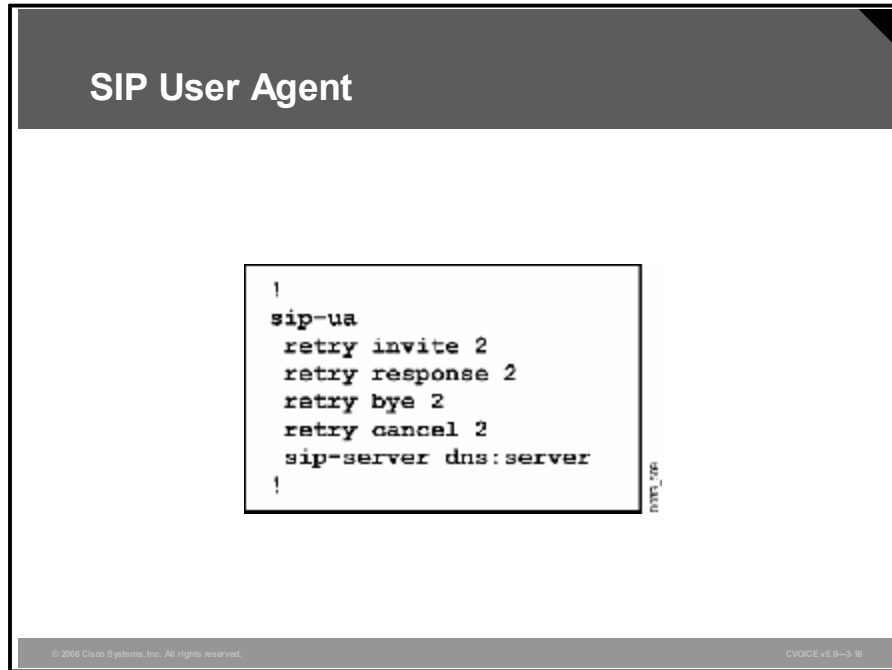
Cisco implements SIP UA (gateway) support in these devices:

- Cisco voice-enabled routers (first available in Cisco IOS Release 12.1)
- Cisco PGW 2200 PSTN Gateways
- Voice-enabled Cisco AS5xx0 universal access servers
- Cisco BTS 10200 Softswitch

- **Network servers:** Cisco implements SIP proxy and redirect server support in the Cisco SIP Proxy Server. The server is an application designed for a Red Hat Linux 7.3 or Solaris 8 operating environment.
- **Other support:** Cisco PIX Security Appliance and Cisco ASA monitor the SIP handshaking to dynamically open conduits for the RTP sessions.

Configuring SIP on a Cisco Router

A SIP configuration consists of two parts: the SIP UA and the VoIP dial peers that select SIP as the session protocol. This topic illustrates and describes the configuration commands that you must use to implement SIP call setup models.



The SIP UA is one part of the SIP configuration. The figure shows an example of a SIP UA configuration.

Example: Configuring a SIP User Agent

The UA is enabled with the **sip-ua** command. Subcommands are optional. The example shows how you can change the value of four retry counters. The configuration also specifies the name of a SIP proxy or redirect server.

SIP Dial Peers

```
!
dial-peer voice 444 voip
 destination-pattern 2339000
 session protocol sipv2
 session target ipv4:172.18.132.205
!
dial-peer voice 111 voip
 destination-pattern 111
 session protocol sipv2
 session target sip-server
!
```

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-3-17

SIP is selected as the call control protocol from inside a dial peer. SIP is requested by the **session protocol sipv2** dial-peer subcommand. The example illustrates two dial-peer variations.

Example: SIP Dial Peers

In the example, both dial peers include the **session protocol sipv2** subcommand, and SIP is used when the destination pattern matches either dial peer. The session target distinguishes one session from the other.

In dial-peer 444, the IP address of the server is provided as the session target. The address can be the address of a UA, proxy server, or redirect server.

In dial-peer 111, the session target is the **sip-server parameter**. When the **sip-server parameter** is the target, the IP address of the actual server is taken from the **sip-server** subcommand in the SIP UA configuration. This means that from global configuration mode, the network administrator has entered the **sip-ua** command and the **sip-server dns:server** subcommand. The address represents the location of a proxy server or redirect server. In this example, the name of the SIP server is “server”.

Monitoring and Troubleshooting

This topic lists the **show** and **debug** commands used to provide support for monitoring and troubleshooting SIP.

Example: show Commands

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP :ENABLED
SIP User Agent for TCP :ENABLED
SIP max-forwards : 6

Router# show sip-ua timers

SIP UA Timer Values (milliseconds)
trying 500, expires 180000, connect 500, disconnect 500
```

© 2006 Cisco Systems, Inc. All rights reserved.VOICE vs.0-3-16

The **show** commands listed here are valuable when examining the status of SIP components and troubleshooting:

- **show call active voice [brief]:** Displays the status, statistics, and parameters for all active voice calls
- **show call history voice [last *n* | record | brief]:** Displays call records from the history buffer
- **show sip-ua retry:** Displays the SIP protocol retry counts (High counts should be investigated.)
- **show sip-ua statistics:** Displays the SIP UA response, traffic, and retry statistics
- **show sip-ua status:** Displays the SIP UA listener status, which should be enabled (shown in the figure)
- **show sip-ua timers:** Displays the current value of the SIP UA timers (shown in the figure)

The **debug** commands listed here are valuable when examining the status of SIP components and troubleshooting:

- **debug voip ccapi inout:** This command shows every interaction with the call control application programming interface (API) on both the telephone interface and on the VoIP side. By monitoring the output, you can follow the progress of a call from the inbound interface or VoIP peer to the outbound side of the call. This **debug** command is very active; you must use it sparingly in a live network.
- **debug ccsip all:** This command enables all **ccsip**-type debugging. This **debug** command is very active; you must use it sparingly in a live network.
- **debug ccsip calls:** This command displays all SIP call details as they are updated in the SIP call control block. You must use this **debug** command to monitor call records for suspicious clearing causes.
- **debug ccsip errors:** This command traces all errors encountered by the SIP subsystem.
- **debug ccsip events:** This command traces events, such as call setups, connections, and disconnections. An events version of a **debug** command is often the best place to start, because detailed debugs provide a great deal of useful information.
- **debug ccsip messages:** This command shows the headers of SIP messages that are exchanged between a client and a server.
- **debug ccsip states:** This command displays the SIP states and state changes for sessions within the SIP subsystem.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **SIP uses IETF protocols, including URL, DNS, and TRIP to define aspects of VoIP and multimedia sessions.**
- **The two basic components of SIP are UAs and network servers.**
- **SIP uses a request/response messaging model for communication. All messages are text-based and modeled on the HTTP syntax.**
- **SIP addresses follow the format and structure of a URL. Network components such as location and registrar servers record addresses and perform address resolution.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-3-18

Summary (Cont.)

- **Call setup between UAs is possible, but a proxy or redirect server may be used for scalability or to simplify UA configuration.**
- **Multiple SIP proxy or redirect servers enhance reliability.**
- **Cisco supports standalone clients and gateway clients. Support for SIP proxy or redirect services is provided by the Cisco SIP Proxy Server.**
- **The sip-ua command can be used to configure SIP on a Cisco router.**
- **Several show and debug commands help in monitoring and troubleshooting SIP.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-3-20

References

For additional information, refer to these resources:

- IETF RFC 3261, *SIP: Session Initiation Protocol*.
<http://www.faqs.org/rfcs/rfc3261.html>.
- *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.
- *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2*.
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080080c8b.html.

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 3-2: Configuring VoIP with SIP

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 IETF protocol does SIP use for call routing?
- A) BGP
 - B) OSPF
 - C) RIP
 - D) TRIP
- Q2) Which SIP service selects the media type and parameters?
- A) user location services
 - B) user capabilities services
 - C) user availability services
 - D) call setup services
 - E) call handling services
- Q3) What are four SIP servers? (Choose four.)
- A) registrar
 - B) gateway
 - C) redirect
 - D) location
 - E) proxy
- Q4) Which SIP server is often colocated with the location server?
- A) proxy
 - B) redirect
 - C) registrar
 - D) gateway
- Q5) Which SIP message is used to provide information to a network server?
- A) INVITE
 - B) ACK
 - C) OPTIONS
 - D) REGISTER
- Q6) Which SIP response message is provisional?
- A) 1xx: Informational
 - B) 2xx: Successful
 - C) 3xx: Redirection
 - D) 4xx: Client error
 - E) 5xx: Server error
 - F) 6xx: Global failure
- Q7) What are three ways in which a SIP UA can resolve an address? (Choose three.)
- A) uses a local host table
 - B) uses **rwhois**
 - C) lets the network server resolve it
 - D) relies on WINS

- Q8) What type of SIP address is represented by “sip:19193631234@gateway.com;user=phone”?
- A) fully qualified domain name
 - B) E.164 address
 - C) mixed address
 - D) URL address
- Q9) What is a disadvantage of the direct call setup method?
- A) It relies on cached information, which may be out of date.
 - B) It uses more bandwidth because it requires more messaging.
 - C) It must learn the coordinates of the destination UA.
 - D) It needs the assistance of a network server.
- Q10) Which statement is true regarding call setup using a proxy server?
- A) If the proxy server fails, the UA uses RTP to establish its sessions.
 - B) If the proxy server fails, the UA cannot establish its own sessions.
 - C) The proxy server sends fewer redirection messages than a redirect server.
 - D) The UAs establish RTP sessions through the proxy server.
- Q11) Which three SIP components need to be replicated to provide fault tolerance? (Choose three.)
- A) proxy server
 - B) redirect server
 - C) registrar server
 - D) location server
 - E) gateway server
- Q12) What method can you use to replicate a proxy server?
- A) configure two replication servers on the network
 - B) configure a redirect server to act as a proxy server
 - C) enable the UA to dynamically locate an active server
 - D) use HSRP
- Q13) Cisco provides support for which three SIP components? (Choose three.)
- A) SIP user agent
 - B) SIP proxy server
 - C) SIP redirect server
 - D) SIP location server
- Q14) With which operating environments can Cisco SIP Proxy Server be used?
- A) Red Hat Linux 7.3 or later
 - B) Windows NT
 - C) Solaris 2.8
 - D) Mac OS
- Q15) Which command is required to enable SIP on a Cisco router?
- A) **sip-ua** interface configuration subcommand
 - B) **sip-ua** dial-peer configuration subcommand
 - C) **sip-ua** global configuration command
 - D) No special command is required. SIP is on by default.

- Q16) What does the **session target sip-server** dial-peer subcommand do?
- A) It tells the router to use DNS to resolve **sip-server**.
 - B) It tells the router to use the server identified in the SIP UA configuration.
 - C) It tells the router to use SIP as the session protocol.
 - D) This is invalid syntax, and an error will be generated.
- Q17) Which **show** command displays SIP UA response and retry information?
- A) **show sip-ua retry**
 - B) **show sip-ua statistics**
 - C) **show call active voice**
 - D) **show sip-ua status**
- Q18) Which **debug** command would you use to trace call setups, connections, and disconnections?
- A) **debug voip ccapi inout**
 - B) **debug ccsip calls**
 - C) **debug ccsip states**
 - D) **debug ccsip messages**
 - E) **debug ccsip events**

Lesson Self-Check Answer Key

- Q1) D
Relates to: Session Initiation Protocol
- Q2) B
Relates to: Session Initiation Protocol
- Q3) A, C, D, E
Relates to: Components of SIP
- Q4) C
Relates to: Components of SIP
- Q5) D
Relates to: SIP Messages
- Q6) A
Relates to: SIP Messages
- Q7) A, B, C
Relates to: SIP Addressing
- Q8) B
Relates to: SIP Addressing
- Q9) A
Relates to: Call Setup Models
- Q10) B
Relates to: Call Setup Models
- Q11) A, B, D
Relates to: Robust Design
- Q12) C
Relates to: Robust Design
- Q13) A, B, C
Relates to: Cisco Implementation of SIP
- Q14) A
Relates to: Cisco Implementation of SIP
- Q15) C
Relates to: Configuring SIP on a Cisco Router
- Q16) B
Relates to: Configuring SIP on a Cisco Router
- Q17) B
Relates to: Monitoring and Troubleshooting
- Q18) E
Relates to: Monitoring and Troubleshooting

Lesson 5

Configuring MGCP

Overview

The Media Gateway Control Protocol (MGCP) environment is an example of a centralized call control model. This lesson describes how to configure MGCP on a gateway, and describes the features and functions of the MGCP environment.

Relevance

An understanding of the features and functions of MGCP, its components, and the relationships that the components establish with each other is important to implement a scalable, resilient, and secure MGCP environment.

Objectives

Upon completing this lesson, you will be able to configure, monitor, and troubleshoot MGCP on a Cisco router. This ability includes being able to meet these objectives:

- Define MGCP and its functions
- Describe the role of each of the basic components of MGCP
- Explain how identifiers are associated with each of the eight types of MGCP endpoints as defined in RFC 2705
- Name seven types of MGCP gateways that are defined in RFC 2705, and identify their functions
- Define the function of a call agent in an MGCP environment
- List the basic concepts of MGCP
- List the steps that are involved in the process of MGCP call establishment
- List MGCP control messages that are used to control and manage endpoints and their connections
- Describe MGCP call setup and control procedures
- Describe design strategies that are used to provide reliability in an MGCP environment
- Describe how Cisco provides support for MGCP components
- Configure an MGCP residential and trunk gateway on a Cisco router
- Monitor MGCP components

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- An understanding of the objectives and principles of signaling and call control in the context of VoIP

Outline

The outline lists the topics included in this lesson.

Outline

- **Overview**
- **MGCP and Its Associated Standards**
- **Basic MGCP Components**
- **MGCP Endpoints**
- **MGCP Gateways**
- **MGCP Call Agents**
- **Basic MGCP Concepts**
- **MGCP Calls and Connections**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-2

Outline (Cont.)

- **MGCP Control Commands**
- **Call Flows**
- **Robust Design**
- **Cisco Implementation of MGCP**
- **Configuring MGCP**
- **Monitoring and Troubleshooting**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-3

MGCP and Its Associated Standards

MGCP controls telephony gateways from a centralized call agent. This topic describes MGCP and identifies its associated standards.

MGCP and Associated Standards

- **MGCP defined in RFC 2705, October 1999**
- **MGCP architecture and requirements defined in RFC 2805, April 2000**
- **Centralized device control with simple endpoints for basic and enhanced telephony services**
 - **Allows remote control of various devices**
 - **Stimulus protocol**
 - **Endpoints and gateways cannot function alone**
- **Uses IETF SDP**
- **Addressing by E.164 telephone number**

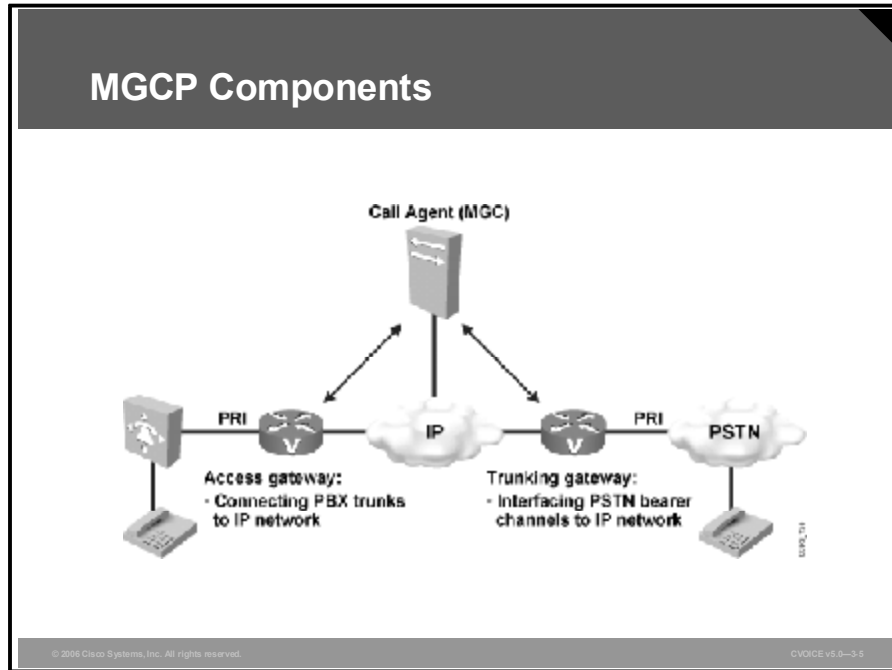
© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-2-4

MGCP defines an environment for controlling telephony gateways from a centralized call control component known as a call agent. An MGCP gateway handles the translation of audio between the telephone switched circuit network (SCN) and the packet-switched network of the Internet. Gateways interact with a call agent that performs signaling and call processing.

Internet Engineering Task Force (IETF) RFC 2705 defines MGCP. RFC 2805 defines an architecture for MGCP. These IETF standards describe MGCP as a centralized device control protocol with simple endpoints. The MGCP protocol allows a central control component, or call agent, to remotely control various devices. This protocol is referred to as a stimulus protocol because the endpoints and gateways cannot function alone. MGCP incorporates the IETF Session Description Protocol (SDP) to describe the type of session to initiate.

Basic MGCP Components

MGCP defines a number of components and concepts. You must understand the relationships between components and how the components use the concepts to implement a working MGCP environment. This topic describes the basic MGCP components.



Here are the components that are used in an MGCP environment:

- **Endpoints:** Represent the point of interconnection between the packet network and the traditional telephone network
- **Gateways:** Handle the translation of audio between the SCN and the packet network
- **Call agent:** Exercises control over the operation of a gateway

The figure shows an MGCP environment with all three components.

Example: Cisco MGCP Components

Cisco voice gateways can act as MGCP gateways. Cisco CallManager acts as an MGCP call agent.

MGCP Endpoints

This topic lists the standard endpoints and defines the way that identifiers are associated with an endpoint.

Endpoints

Eight types of endpoints are defined in RFC 2705:

- **Digital channel**
- **Analog line**
- **Announcement server access point**
- **IVR access point**
- **Conference bridge access point**
- **Packet relay**
- **Wiretap access point**
- **ATM trunk side interface**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-5

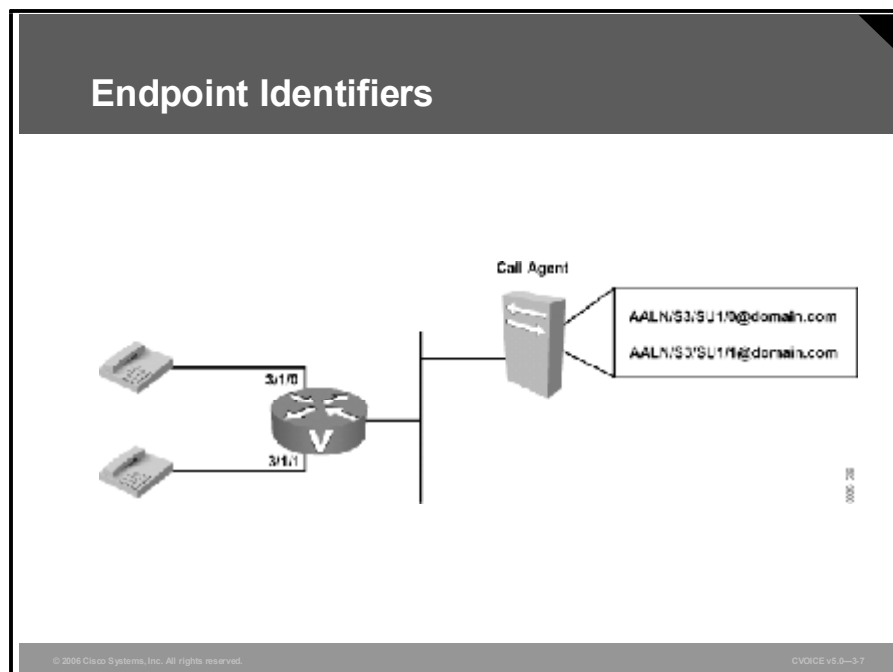
Endpoints represent the point of interconnection between the packet network and the traditional telephone network. Endpoints can be physical, representing a Foreign Exchange Station (FXS) port or a channel in a T1 or E1, or they can be logical, representing an attachment point to an announcement server.

To manage an endpoint, the call agent must recognize the characteristics of an endpoint. To aid in this process, endpoints are categorized into several types. The intent is to configure a call agent to manage a type of endpoint rather than to manage each endpoint individually.

There are several types of endpoints. RFC 2705 defines eight types, as follows:

- **Digital service level zero (DS0):** This type of endpoint represents a single channel (DS0) in the digital hierarchy. A digital channel endpoint supports more than one connection.
- **Analog line:** This type of endpoint represents the client side interface, such as FXS, or switch side interface, such as Foreign Exchange Office (FXO), to the traditional telephone network. An analog line endpoint supports more than one connection.
- **Announcement server access point:** This type of endpoint represents access to an announcement server, for example, to play recorded messages. An announcement server endpoint may have only one connection. Multiple users of the announcement server are modeled to use different endpoints.
- **Interactive voice response (IVR) access point:** An IVR access point represents access to an IVR service. An IVR endpoint has one connection. Multiple users of the IVR system are modeled to use different endpoints.

- **Conference bridge access point:** This type of access point represents access to a specific conference. Each conference is modeled as a distinct endpoint. A conference bridge endpoint supports more than one connection.
- **Packet relay:** This type of endpoint represents access that bridges two connections for interconnecting incompatible gateways or relaying them through a firewall environment. A packet relay endpoint has two connections.
- **Wiretap access point:** A wiretap access point represents access for recording or playing back a connection. A wiretap access point endpoint has one connection.
- **ATM trunk side interface:** An ATM trunk side interface represents a single instance of an audio channel in the context of an ATM network. An ATM interface supports more than one connection.



When interacting with a gateway, the call agent directs its commands to the gateway for the express purpose of managing an endpoint or a group of endpoints. An endpoint identifier, as its name suggests, identifies endpoints.

Endpoint identifiers consist of two parts: a local name of the endpoint in the context of the gateway and the domain name of the gateway itself. The two parts are separated by an “at” sign (@). If the local part represents a hierarchy, the subparts of the hierarchy are separated by a slash (/). In the graphic, the local ID may be representative of a particular “gateway/circuit #”, and the “circuit #” may in turn be representative of a “circuit ID/channel #”.

Example: Endpoint Identifiers

In the figure, “mgcp.gateway.cisco.com” is the domain name and “t1toSJ/17” refers to channel 17 in the T1 to San Jose.

MGCP Gateways

This topic lists several standard gateways and describes their functions.

Gateways and Their Roles

- **Trunk gateway SS7 ISUP**
- **Trunk gateway MF**
- **NAS**
- **Combined NAS-VoIP gateway**
- **Access gateway**
- **Residential gateway**
- **Announcement servers**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-3-5

Gateways are clustering points for endpoints. Gateways handle the translation of audio between the SCN and the packet network.

Although gateways are implemented in real systems, from a modeling point of view, gateways are logical components. In this context, gateways represent a clustering of a single type and profile of endpoints.

A gateway interacts with one call agent only; therefore, it associates with one call agent at a time.

RFC 2705 identifies these seven types of gateways:

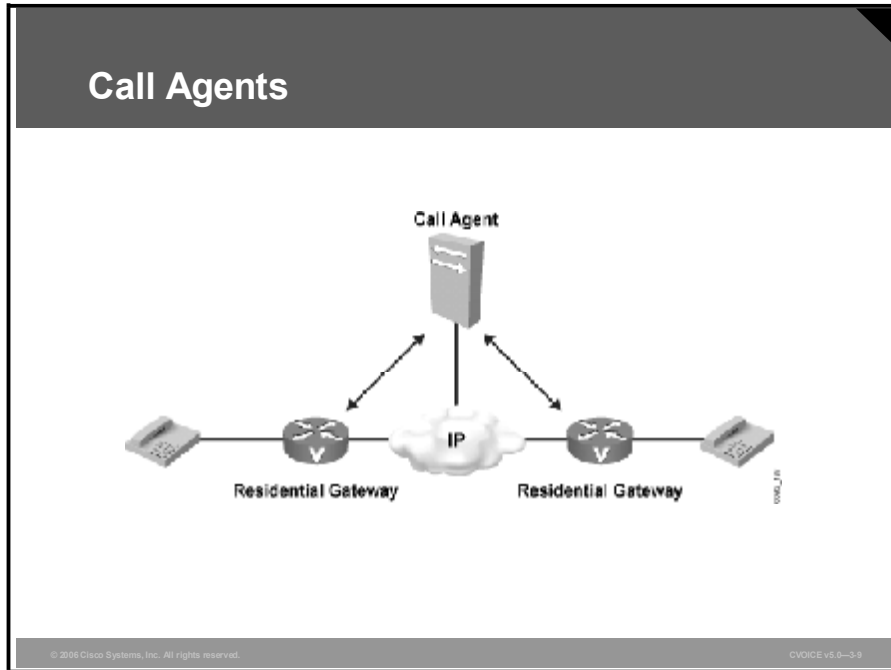
- **Trunk gateway Signaling System 7 (SS7) ISDN User Part (ISUP):** Supports digital circuit endpoints subject to ISDN signaling
- **Trunk gateway multifrequency (MF):** Typically supports digital or analog circuit endpoints that are connected to a service provider of an enterprise switch that is subject to MF signaling
- **Network access server (NAS):** Supports an interconnect to endpoints over which data (modem) applications are provided
- **Combined NAS-Voice over IP (VoIP) gateway:** Supports an interconnect to endpoints over which a combination of voice and data access is provided

- **Access gateway:** Supports analog and digital endpoints connected to a PBX
- **Residential gateway:** Supports endpoints connected to traditional analog interfaces
- **Announcement servers:** Supports endpoints that represent access to announcement services

Multiple gateway types, and multiple instances of the same type, can be incorporated into a single physical gateway implementation.

MGCP Call Agents

This topic describes how a call agent controls gateways and endpoints.



A call agent, or Media Gateway Controller (MGC), represents the central controller in an MGCP environment.

A call agent exercises control over the operation of a gateway and its associated endpoints by requesting that a gateway observe and report events. In response to the events, the call agent instructs the endpoint what signal, if any, the endpoint should send to the attached telephone equipment. This requires a call agent to recognize each endpoint type that it supports and the signaling characteristics of each physical and logical interface that is attached to a gateway.

A call agent uses its directory of endpoints, and the relationship that each endpoint has with the dial plan, to determine call routing. Call agents initiate all VoIP call legs.

Basic MGCP Concepts

This topic introduces the basic MGCP concepts.

Basic MGCP Concepts

- **Calls and connections**
- **Events and signals**
- **Packages and digit maps**

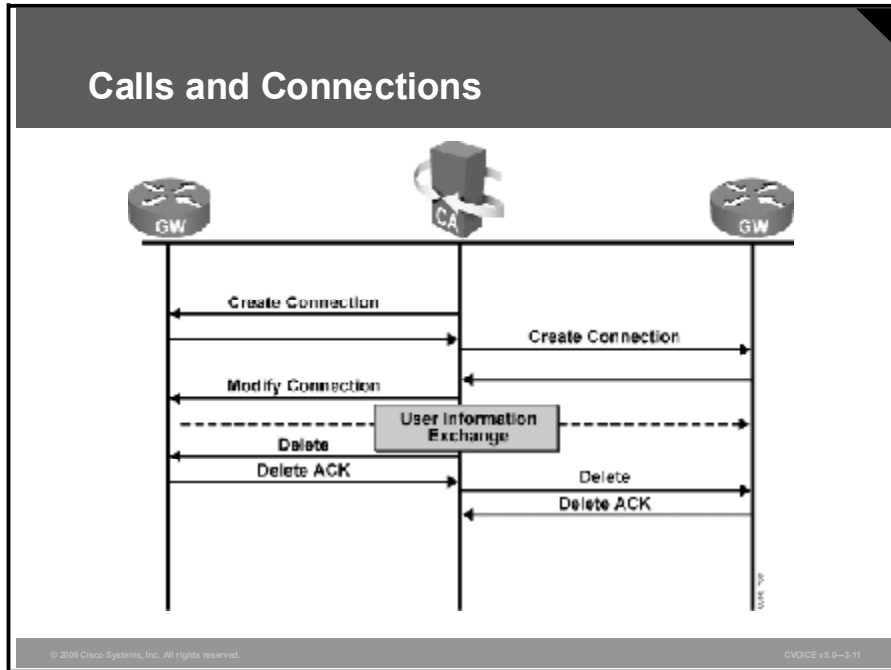
© 2006 Cisco Systems, Inc. All rights reserved. VOICE vs.0-3-10

The basic MGCP concepts are listed here:

- **Calls and connections:** Allow end-to-end calls to be established by connecting two or more endpoints
- **Events and signals:** Fundamental MGCP concept that allows a call agent to provide instructions for the gateway
- **Packages and digit maps:** Fundamental MGCP concept that allows a gateway to determine the call destination

MGCP Calls and Connections

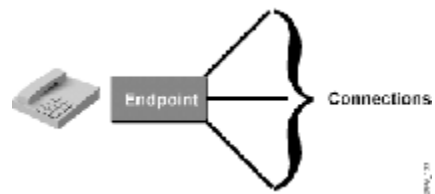
This topic discusses how end-to-end calls are established by connecting multiple endpoints.



End-to-end calls are established by connecting two or more endpoints. To establish a call, the call agent instructs the gateway that is associated with each endpoint to make a connection with a specific endpoint or an endpoint of a particular type. The gateway returns the session parameters of its connection to the call agent, which in turn sends these session parameters to the other gateway. With this method, each gateway acquires the necessary session parameters to establish Real-Time Transport Protocol (RTP) sessions between the endpoints. All connections that are associated with the same call will share a common Call ID and the same media stream.

At the conclusion of a call, the call agent sends a DeleteConnection (DLCX) request to each gateway.

Multipoint Calls



To create a multipoint call, the call agent instructs an endpoint to create multiple connections. The endpoint is responsible for mixing audio signals.

MGCP Control Messages

MGCP defines nine messages to control and manage endpoints and their connections. This topic describes these control messages.

Control Commands

- **EndpointConfiguration (EPCF)**
- **NotificationRequest (RQNT)**
- **Notify (NTFY)**
- **CreateConnection (CRCX)**
- **ModifyConnection (MDCX)**
- **DeleteConnection (DLCX)**
- **AuditEndpoint (AUEP)**
- **AuditConnection (AUCX)**
- **RestartInProgress (RSIP)**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-213

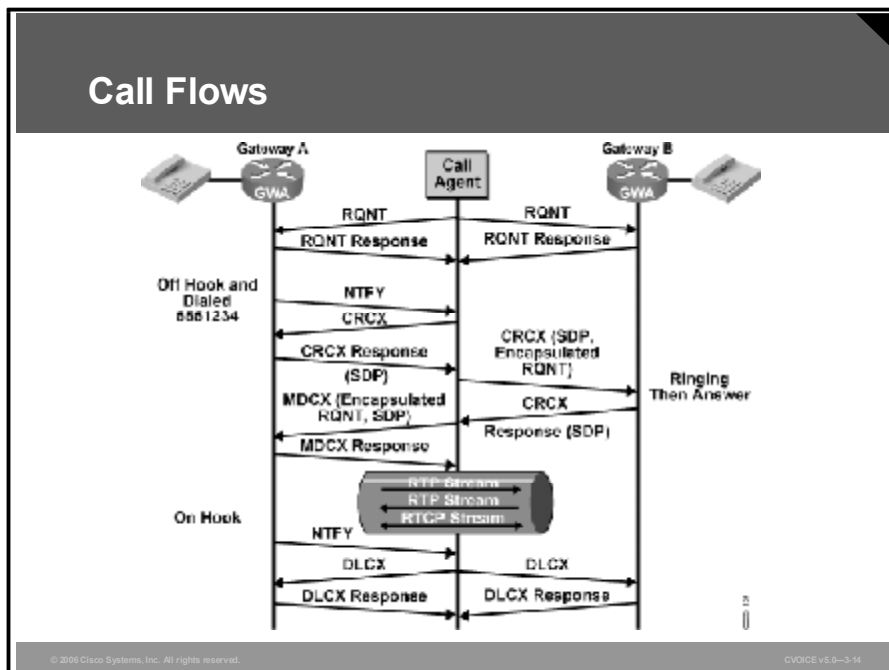
A call agent uses control messages to direct its gateways and their operational behavior. Gateways use the control messages listed here in responding to requests from a call agent and notifying the call agent of events and abnormal behavior:

- **EndpointConfiguration (EPCF):** This message identifies the coding characteristics of the endpoint interface on the line side of the gateway. The call agent issues the command.
- **NotificationRequest (RQNT):** This message instructs the gateway to watch for events on an endpoint and the action to take when they occur. The call agent issues the command.
- **Notify (NTFY):** This message informs the call agent of an event for which notification was requested. The gateway issues the command.
- **CreateConnection (CRCX):** This message instructs the gateway to establish a connection with an endpoint. The call agent issues the command.
- **ModifyConnection (MDCX):** This message instructs the gateway to update its connection parameters for a previously established connection. The call agent issues the command.
- **DeleteConnection (DLCX):** This message informs the recipient to delete a connection. The call agent or the gateway can issue the command. The gateway or the call agent issues the command to advise that it no longer has the resources to sustain the call.
- **AuditEndpoint (AUEP):** This message requests the status of an endpoint. The call agent issues the command.
- **AuditConnection (AUCX):** This message requests the status of a connection. The call agent issues the command.

- **RestartInProgress (RSIP):** This message notifies the call agent that the gateway and its endpoints are removed from service or are being placed back in service. The gateway issues the message.

Call Flows

This topic illustrates and explains the interactions between a call agent and its associated gateways.



The figure illustrates a dialog between a call agent and two gateways. Although the gateways in this example are both residential gateways, the principles of operation listed here are the same for other gateway types:

1. The call agent sends an RQNT 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 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 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 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 an NTFY 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.
5. After confirming that a call is possible based on the dialed digits, the call agent instructs gateway A to create a connection (CRCX) with its endpoint.

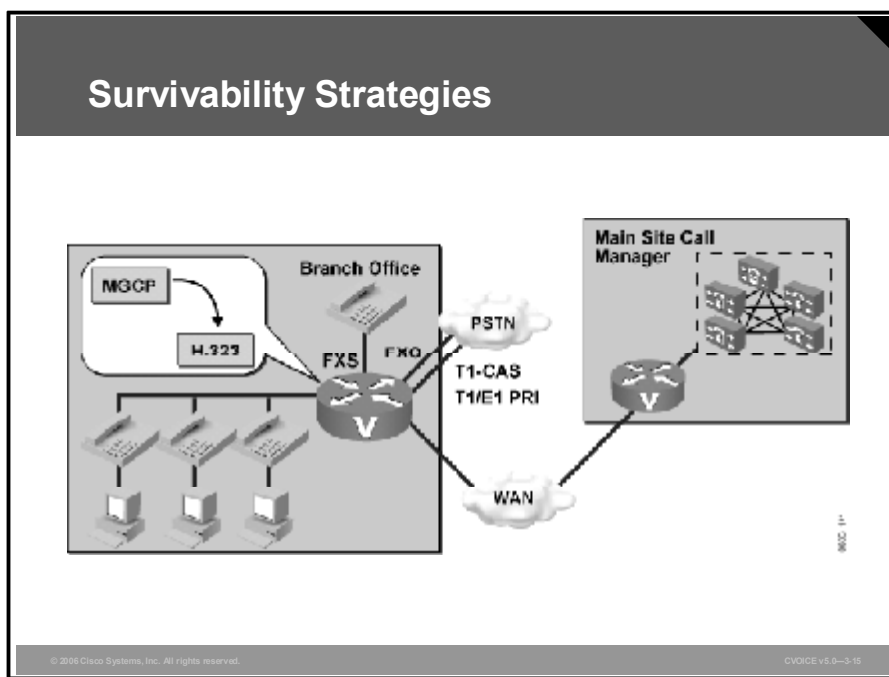
6. The gateway responds with a session description if it is able to accommodate the connection. The session description identifies at least the IP address and User Datagram Protocol (UDP) port for use in a subsequent RTP session. The gateway does not have a session description for the remote side of the call, and the connection enters a wait state.
7. The call agent prepares and sends a connection request 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. 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. This request may contain an encapsulated NTFY 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 respond.

Robust Design

Maintaining high availability in an MGCP environment requires a design that accommodates the failure of a call agent. This topic describes two strategies for managing the loss of a call agent.



In the MGCP environment, the call agent controls all call setup processing on the IP and the telephony sides of a gateway. Because a gateway is associated with only one call agent at a time, if that call agent fails or is inaccessible for any reason, the gateway and its endpoints are left uncontrolled and, for all practical purposes, useless. Cisco Systems has developed two methods to handle lost communication between a call agent and its gateways: MGCP switchover and switchback, and MGCP gateway fallback. These features operate in the manner described here:

- **MGCP switchover and switchback:** MGCP switchover permits the use of redundant MGCP call agents. This feature requires two or more Cisco CallManager servers to operate as MGCP call agents. One Cisco CallManager server becomes the primary server and functions as the MGCP call agent. The other Cisco CallManager servers remain available as backup servers.

The MGCP gateway monitors MGCP messages sent by the Cisco CallManager server. If traffic is undetected, the gateway transmits keepalive packets to which the Cisco CallManager server responds. If the gateway does not detect packets from the Cisco CallManager server for a specified period, it tries to establish a new connection with a backup Cisco CallManager server.

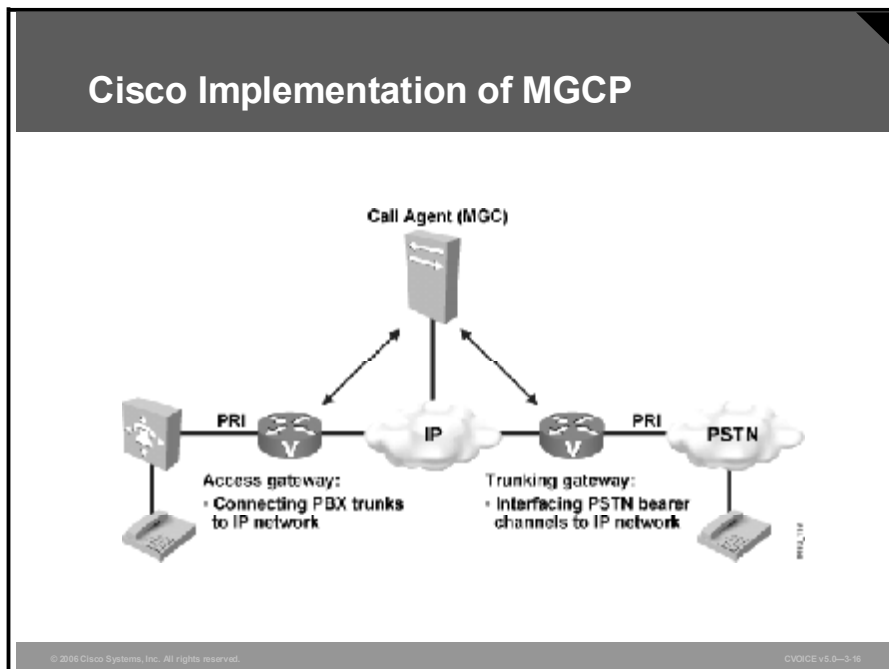
You can configure a Cisco voice gateway to reestablish connection with the primary Cisco CallManager server when it becomes available again. This is the switchback function.

- **MGCP gateway fallback:** MGCP gateway fallback is a feature that improves the reliability of MGCP branch networks. A WAN link connects the MGCP gateway at the remote site to the Cisco CallManager server at the central sites (the MGCP call agent). If the WAN link fails, the fallback feature keeps the gateway working as an H.323 gateway.

MGCP gateway fallback works in conjunction with the Survivable Remote Site Telephony (SRST) feature. SRST allows Cisco gateways and routers to manage connections temporarily for Cisco IP Phones when a connection to a Cisco CallManager server is unavailable.

Cisco Implementation of MGCP

This topic describes how Cisco implements MGCP.



Cisco provides support for MGCP gateways and the call agent as follows:

- **Gateways:** Cisco implements MGCP trunk gateway and residential gateway support in these devices:
 - Cisco voice-enabled routers (first available in Cisco IOS Release 12.1)
 - Cisco PGW 2200 Public Switched Telephone Network (PSTN) Gateways
 - Cisco Voice Gateway 224 (VG224)
 - Voice-enabled Cisco AS5xx0 universal access servers
 - Cisco BTS 10200 Softswitch

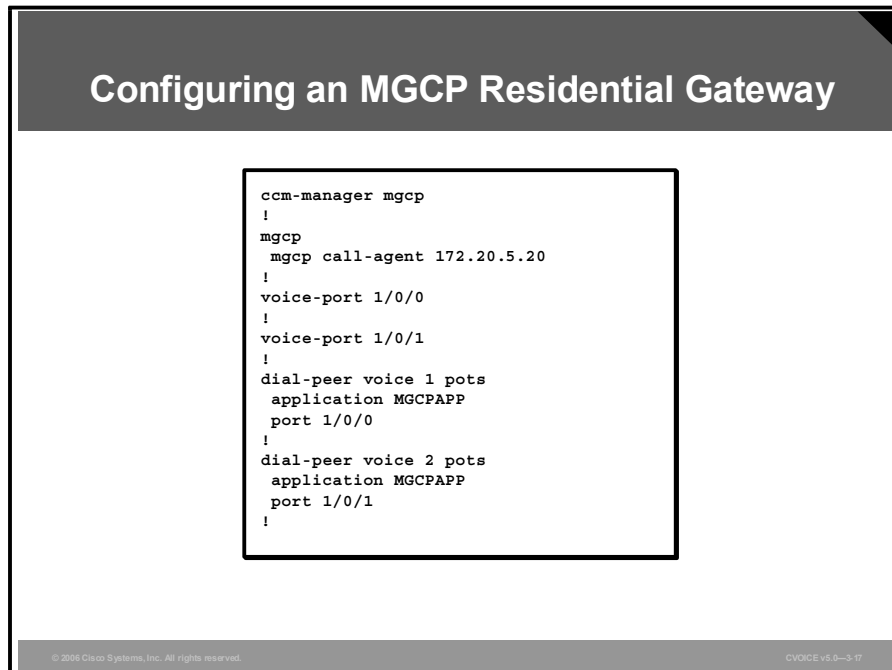
Note Cisco CallManager interworking requires Cisco IOS Release 12.2.

- **Call agent:** Cisco implements call agent support in these applications:
 - Cisco CallManager
 - Cisco BTS 10200 Softswitch

Note Residential gateway and trunk gateway support does *not* include all analog and digital signaling types on the telephone interfaces. Check Cisco.com for an up-to-date list.

Configuring MGCP

This topic illustrates the configuration commands that are required to implement MGCP residential gateway and trunk gateway capabilities on a Cisco router.



The figure highlights the commands required to configure an MGCP residential gateway.

MGCP is invoked with the **mgcp** command. If the call agent expects the gateway to use the default port (UDP 2427), the **mgcp** command is used without any parameters. If the call agent requires a different port, the port must be configured as a parameter in the **mgcp** command; for example, **mgcp 5036** would tell the gateway to use port 5036 instead of the default port.

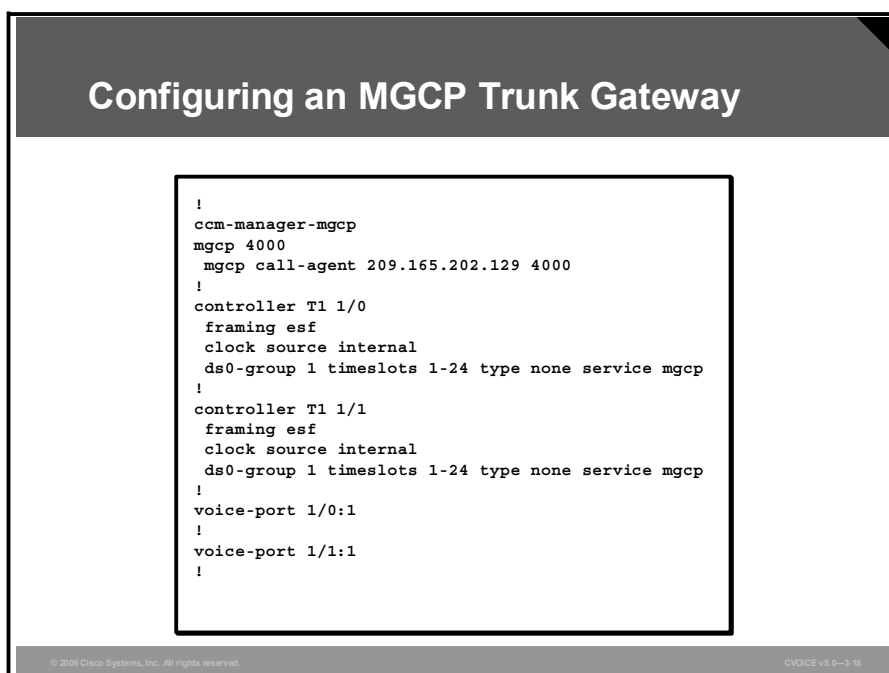
At least one **mgcp call-agent** command is required below the **mgcp** command. This command indicates the location of the call agent. The command identifies the call agent by an IP address or a host name. Using a host name adds a measure of fault tolerance in a network that has multiple call agents. When the gateway asks the Domain Name System (DNS) for the IP address of the call agent, the DNS may provide more than one address, in which case the gateway can use either one. If multiple instances of the **mgcp call-agent** command are configured, the gateway uses the first call agent to respond.

Other **mgcp** subcommands are optional.

Example: MGCP Residential Gateway Configuration

In the example, the configuration identifies the packages that the gateway expects the call agent to use when it communicates with the gateway. The last **mgcp** command specifies the default that the gateway uses if the call agent does not share the capabilities. In this example, the command is redundant because the line package is the default for a residential gateway.

When the parameters of the MGCP gateway are configured, the active voice ports (endpoints) are associated with the MGCP. Dial peer 1 illustrates an **application mgcpapp** subcommand. This command binds the voice port (“1/0/0” in this case) to the MGCP. Also, notice that the dial peer does not have a destination pattern. A destination pattern is not used because the relationship between the dial number and the port is maintained by the call agent.



Note The **ccm-manager-mgcp** command is required only if the call agent is a Cisco CallManager.

The second example illustrates the configuration of a trunk gateway.

Configuring trunk gateways requires the address or the name of the call agent, which is a requirement common to a residential gateway (RGW). The trunk package is the default for a trunk gateway and does not need to be configured. Again, other parameters are optional.

Example: Configuring an MGCP Trunk Gateway

The figure illustrates commands for configuring a trunk gateway. Instead of using the **application mgcpapp** command in a dial peer, a trunk endpoint identifies its association with MGCP using the **service mgcp** parameter in the **ds0-group** controller subcommand. As always in MGCP, the call agent maintains the relationship between the endpoint (in this case, a digital trunk) and its address.

Monitoring and Troubleshooting

Several **show** and **debug** commands provide support for monitoring and troubleshooting MGCP. This topic lists many useful **show** and **debug** commands.

Example: show Command

```
Router# show mgcp statistics

UDP pkts rx 8, tx 9
Unrecognized rx pkts 0, MGCP message parsing errors 0
Duplicate MGCP ack tx 0, Invalid versions count 0
CreateConn rx 4, successful 0, failed 0
DeleteConn rx 2, successful 2, failed 0
ModifyConn rx 4, successful 4, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 4, failed 0
AuditConnection rx 0, successful 0, failed 0
AuditEndpoint rx 0, successful 0, failed 0
RestartInProgress tx 1, successful 1, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 8, NACK tx 0
ACK rx 0, NACK rx 0
IP address based Call Agents statistics:
IP address 10.24.167.3, Total msg rx 8, successful 8,
failed 0
```

The figure illustrates the output of one of the **show** commands. The **show** and **debug** commands are valuable for examining the current status of the MGCP components and for troubleshooting. You should be familiar with the information provided from each command and how this information can help you.

The **show** commands listed here are useful for monitoring and troubleshooting MGCP:

- **show call active voice [brief]:** This command displays the status, statistics, and parameters for all active voice calls. When the call is disconnected, this information is transferred to the history records.
- **show call history voice [last n | record | brief]:** This command displays call records from the history buffer.
- **show mgcp:** This command displays basic configuration information about the gateway.
- **show mgcp connection:** This command displays details of the current connections.
- **show mgcp endpoint:** This command displays a list of the voice ports that are configured for MGCP.
- **show mgcp statistics:** This command displays a count of the successful and unsuccessful control commands (shown in the figure). You should investigate a high unsuccessful count.

These **debug** commands are useful for monitoring and troubleshooting MGCP:

- **debug voip ccapi inout:** This command shows every interaction with the call control application programming interface (API) on the telephone interface and the VoIP side. Watching the output allows users to follow the progress of a call from the inbound interface or VoIP peer to the outbound side of the call. This **debug** command is very active; you must use it sparingly in a live network.
- **debug mgcp [all | errors | events | packets | parser]:** This command reports all **mgcp** command activity. You must use this **debug** command to trace the MGCP request and responses.

Summary

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

Summary

- **MGCP defines an environment for controlling telephony gateways from a centralized call agent.**
- **MGCP components include endpoints, gateways, and call agents.**
- **Calls are created by connecting endpoints. Endpoints can be physical or logical.**
- **MGCP gateways incorporate endpoints, act upon directives issued by a call agent to manage the telephony interface, and translate voice signals.**
- **The call agent instructs the MGCP gateway to watch for events and provides signaling on its telephony interfaces.**
- **Calls and connections are basic concepts in MGCP.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-3.20

Summary (Cont.)

- **During call setup, the gateway associated with each endpoint makes a connection with a specific endpoint and returns the session parameters to the call agent. The call agent sends these session parameters to the other gateway to establish the call.**
- **A call agent and its gateways exchange requests and responses by way of control commands.**
- **Call flow consists of an exchange of messages between the call agent and the gateway.**
- **MGCP switchover and switchback and MGCP gateway fallback are two strategies for improving availability in an MGCP implementation.**

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-3.21

Summary (Cont.)

- Cisco implements an MGCP call agent in Cisco CallManager. Gateways of various types are implemented by routers or specialized gateway products.
- The mgcp command can be used to configure residential and trunk gateways on a Cisco router.
- Several show and debug commands help to monitor and troubleshoot.

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-3.22

References

For additional information, refer to these resources:

- IETF RFC 2705: *Media Gateway Control Protocol (MGCP), Version 1.0.*
<http://www.faqs.org/rfcs/rfc2705.html>.
- IETF RFC 2805: *Media Gateway Control Protocol Architecture and Requirements.*
<http://www.faqs.org/rfcs/rfc2805.html>.
- *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.
- *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2.*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080080c8b.html.
- *Configure MGCP Gateway and FXO/FXS on a CallManager Server.*
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a008017825e.shtml.

Next Steps

For the associated lab exercise, refer to the following section of the course Lab Guide:

- Lab Exercise 3-3: Configuring VoIP with MGCP

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 call control model is used by MGCP?
- A) distributed
 - B) centralized
 - C) ad hoc
 - D) hybrid
- Q2) Which protocol is used by MGCP to describe the type of session to initiate?
- A) SIP
 - B) CDP
 - C) SDP
 - D) MGC
- Q3) Which MGCP component represents the point of interconnection between the packet network and the traditional telephone network?
- A) endpoint
 - B) gate-array
 - C) gatekeeper
 - D) call agent
- Q4) What is the function of an MGCP gateway?
- A) handles the translation of video between the SCN and packet-switched network
 - B) handles the translation of audio between the SCN and packet-switched network
 - C) controls the operation of the endpoints and the call agent
 - D) only allows authenticated traffic into the network
- Q5) Which type of MGCP endpoint represents an access type that bridges two connections for interconnecting incompatible gateways?
- A) DS0
 - B) analog line
 - C) IVR access point
 - D) packet relay
 - E) wiretap access point
- Q6) Which type of MGCP endpoint can have only one connection?
- A) ATM trunk side interface
 - B) wiretap access point
 - C) analog line
 - D) DS0
 - E) packet relay
- Q7) With how many call agents can an MGCP gateway interact?
- A) one
 - B) two
 - C) seven
 - D) varies

- Q8) Match the type of MGCP gateway with its description.
- A) trunk gateway ISUP
 - B) NAS
 - C) access gateway
 - D) residential gateway
- _____ 1. supports interconnect to endpoints over which data (modem) applications are provided
- _____ 2. supports digital circuit endpoints subject to ISDN signaling
- _____ 3. supports endpoints connected to traditional analog interfaces
- _____ 4. supports analog and digital endpoints connected to a PBX
- Q9) Why does MGCP require the gateway to observe and report events?
- A) so that MGCP can recognize each endpoint that it supports
 - B) so that MGCP can tell the endpoint what type of signal to send to the attached telephone equipment
 - C) so that MGCP can recognize the signaling characteristics of each physical interface attached to the gateway
 - D) so that MGCP can recognize the signaling characteristics of each logical interface attached to the gateway
- Q10) Which two pieces of information does MGCP use to determine call routing? (Choose two.)
- A) its directory of endpoints
 - B) the endpoint type
 - C) the events reports sent by the gateway
 - D) the relationship of endpoints with the dial plan
 - E) the signaling characteristics of the gateway interfaces
- Q11) Which two concepts does MGCP use to determine the destination of a call? (Choose two.)
- A) calls
 - B) connections
 - C) digit maps
 - D) events
 - E) packages
 - F) signals
- Q12) Which two concepts does MGCP use to allow a call agent to provide instructions to a gateway? (Choose two.)
- A) calls
 - B) connections
 - C) digit maps
 - D) events
 - E) packages
 - F) signals

- Q13) Which MGCP component is responsible for mixing audio signals in a multipoint call?
- A) call agent
 - B) MGC
 - C) endpoint
 - D) gateway
- Q14) At the conclusion of an MGCP call, which message does the call agent send to each gateway?
- A) bye request
 - B) cancel request
 - C) disconnect request
 - D) delete connection request
- Q15) Match the MGCP control message with its function.
- A) EndpointConfiguration
 - B) NotificationRequest
 - C) ModifyConnection
 - D) AuditEndpoint
 - E) RestartInProgress
- _____ 1. requests the status of an endpoint
- _____ 2. instructs the gateway on what action to take on the occurrence of an event
- _____ 3. identifies the coding characteristics of the endpoint interface on the line side of the gateway
- _____ 4. notifies the call agent that the gateway and its endpoints are removed from service
- _____ 5. instructs the gateway to update its connection parameters for a previously established connection
- Q16) Which two messages are issued by a gateway? (Choose two.)
- A) EndpointConfiguration
 - B) NotificationRequest
 - C) CreateConnection
 - D) DeleteConnection
 - E) RestartInProgress
- Q17) Which two types of information are included in the NTFY sent by a gateway to the call agent? (Choose two.)
- A) call destination
 - B) endpoint identification
 - C) event identification
 - D) local gatekeeper
 - E) signal type
- Q18) In MGCP calls, when do the gateways delete a connection?
- A) when one user hangs up
 - B) when one endpoint recognizes an on-hook transition
 - C) when the gateway notifies the call agent of an on-hook transition event
 - D) when the call agent instructs the gateways to delete the connection

- Q19) What is the MGCP switchback function?
- A) The gateway establishes a connection with the backup Cisco CallManager server after failing to get packets from the primary Cisco CallManager server.
 - B) The gateway reestablishes a connection with the primary Cisco CallManager server when it becomes available.
 - C) When the WAN link between the gateway and Cisco CallManager server fails, the gateway continues to function as an H.323 gateway.
 - D) Cisco gateways manage connections temporarily when a connection to Cisco CallManager goes down.
- Q20) When Cisco CallManager is unavailable, which feature works with MGCP gateway fallback to manage connections temporarily for Cisco IP Phones?
- A) SRST
 - B) RSVP
 - C) Cisco VG200
 - D) Cisco BTS 10200 Softswitch
- Q21) Which two Cisco applications support the MGCP call agent? (Choose two.)
- A) Cisco voice-enabled routers with Cisco IOS Release 12.1 and later
 - B) Cisco PGW 2200 PSTN Gateways
 - C) Cisco CallManager
 - D) Cisco VG200
 - E) Cisco BTS 10200 Softswitch
- Q22) Which Cisco application does NOT provide residential gateway support?
- A) Cisco CallManager
 - B) Cisco voice-enabled routers with Cisco IOS Release 12.1 and later
 - C) Cisco PGW 2200 PSTN Gateways
 - D) Cisco BTS 10200 Softswitch
- Q23) Which configuration command enables MGCP on UDP port 5000?
- A) **mgcp 5000** global configuration command
 - B) **mgcp udp 5000** global configuration command
 - C) **mgcp 5000** interface configuration subcommand
 - D) **mgcp 2427** global configuration subcommand
- Q24) How do you configure a router to use MGCP on a digital port?
- A) add the **application mgcpapp** subcommand to the dial peer
 - B) add the **service mgcp** subcommand to the dial peer
 - C) add the parameter application **mgcpapp** to the **ds0-group controller** subcommand
 - D) add the **service mgcp** parameter to the **ds0-group controller** subcommand
- Q25) Which two commands display the current MGCP calls? (Choose two.)
- A) **show call active voice**
 - B) **show mgcp endpoints**
 - C) **show mgcp connections**
 - D) **debug mgcp packets**
 - E) **show mgcp statistics**
- Q26) Which command allows you to view the details of every MGCP packet?
- A) **debug voip ccapi inout**
 - B) **show mgcp packets**
 - C) **show call active voice**
 - D) **debug mgcp packets**

Lesson Self-Check Answer Key

- Q1) B
Relates to: MGCP and Its Associated Standards
- Q2) C
Relates to: MGCP and Its Associated Standards
- Q3) A
Relates to: Basic MGCP Components
- Q4) B
Relates to: Basic MGCP Components
- Q5) D
Relates to: MGCP Endpoints
- Q6) B
Relates to: MGCP Endpoints
- Q7) A
Relates to: MGCP Gateways
- Q8) 1-B
2-A
3-D
4-C
Relates to: MGCP Gateways
- Q9) B
Relates to: MGCP Call Agents
- Q10) A, D
Relates to: MGCP Call Agents
- Q11) C, E
Relates to: Basic MGCP Concepts
- Q12) D, F
Relates to: Basic MGCP Concepts
- Q13) C
Relates to: MGCP Calls and Connections
- Q14) D
Relates to: MGCP Calls and Connections
- Q15) 1-D
2-B
3-A
4-E
5-C
Relates to: MGCP Control Messages

- Q16) D, E
Relates to: MGCP Control Messages
- Q17) B, C
Relates to: Call Flows
- Q18) D
Relates to: Call Flows
- Q19) B
Relates to: Robust Design
- Q20) A
Relates to: Robust Design
- Q21) C, E
Relates to: Cisco Implementation of MGCP
- Q22) A
Relates to: Cisco Implementation of MGCP
- Q23) A
Relates to: Configuring MGCP
- Q24) D
Relates to: Configuring MGCP
- Q25) A, C
Relates to: Monitoring and Troubleshooting
- Q26) D
Relates to: Monitoring and Troubleshooting

Lesson 6

Comparing Call Control Models

Overview

This lesson compares the features and functions of the three call control models: H.323, session initiation protocol (SIP), and Media Gateway Control Protocol (MGCP). This lesson also highlights the environments for which each call control model is best suited.

Relevance

Understanding the capabilities of the H.323, SIP, and MGCP models helps you decide which call control model best meets your requirements.

Objectives

Upon completing this lesson, you will be able to determine the best call control model for your network. This ability includes being able to meet these objectives:

- Compare the features and benefits of H.323, SIP, and MGCP
- Describe the environments best suited to H.323, SIP, and MGCP
- Select the appropriate call control models for a given scenario

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- An understanding of the objectives and principles of signaling and call control in the context of VoIP
- An understanding of the H.323, SIP, and MGCP call control models

Outline

The outline lists the topics included in this lesson.

Outline

- **Overview**
- **Feature Comparison Charts**
- **Strengths of H.323, SIP, and MGCP**
- **Selecting Appropriate Call Control**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0-3.2

Feature Comparison Charts

This topic compares the origins, architectures, characteristics, and capabilities of the H.323, SIP, and MGCP call control models.

Components and Services			
	H.323	SIP	MGCP
Common Control Components	Gatekeeper	Proxy Server, Redirect Server, Location Server, Registrar Server	Call Agent
Endpoints	Gateway, Terminal	Client (IP Telephone, Gateway)	Media Gateway (or Gateway)
Call Administration and Accounting	Gateway, Gatekeeper	Gateway	Call Agent
Call Status	Gateway, Gatekeeper	Gateway	Call Agent
Address Management	Gatekeeper	Location Server, Registrar Server	Call Agent
Admission Control	Gatekeeper	Not Supported	Call Agent

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v9.0-3.3

In a generic model, the components of signaling and call control are identified as common control components and endpoints. Common control components provide a set of optional services: call administration and accounting, call status, address management, and admission control. The chart in the figure identifies how the basic components of the generic model are configured in H.323, SIP, and MGCP, and, if applicable, where optional services are provided.

Characteristics

	H.323	SIP	MGCP
Standards Body	ITU-T	IETF	IETF
Architecture	Distributed	Distributed	Centralized
Current Version	H.323v4	SIP 2.0 (RFC 3261)	MGCP 1.0 (RFC 2705)
Signaling Transport	TCP (Call Signaling Channel, H.245 Control Channel) or UDP (RAS Channel)	TCP or UDP	UDP
Multimedia Capable	Yes	Yes	Yes
Call Control Encoding	Abstract Syntax Notation (ASN.1) Basic Encoding Rules (BER)	Text	Text
Supplemental Services	Provided by Endpoints or Call Control	Provided by Endpoints or Call Control	Provided by Call Control

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-34

Note As of version 3 of H.323, the calling signaling channel and the H.245 control channel can operate over User Datagram Protocol (UDP).

The chart in the figure compares several factors that can influence your decision to select H.323, SIP, or MGCP.

Standards Bodies (ITU-T vs. IETF)

The two originating authorities for the model may seem to have little relevance. However, the ITU-T and the Internet Engineering Task Force (IETF) work under different conditions, a fact that has an impact on the results and the speed of their work.

Although the ITU-T is older than the IETF, it is associated with a publishing cycle and consensus process that is often blamed for delay. However, its rigorous procedures result in mature recommendations with the consistent use of language and terminology. The consensus process requires a high level of agreement and is generally accepted as the preferred way to proceed internationally.

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.

Knowing which standards body is involved provides a sense of the standards development process, the pace of work, and the quality of results.

Architecture (Centralized vs. Distributed)

The distinction between the centralized architecture and the distributed architecture can influence which model you choose.

Current Version

The current version of a specification or recommendation is an indication of its maturity.

Signaling Transport (TCP vs. UDP)

Understanding the underlying transport of the signaling channels helps to explain the performance and overheads of the relationship between H.323, SIP, or MGCP components. Connectionless, UDP-based relationships must shift reliability and sequencing into the application, making them more complex. Both reliability and sequencing are built into TCP. However, UDP-based applications are designed to respond more quickly than TCP-based applications. This is significant, for example, during call setup.

Multimedia Capability (Yes or No)

The ability to transport information of different types, such as audio, video, and data, can be a determining factor in choosing between H.323, SIP, or MGCP.

Call Control Encoding (ASN.1 vs. Text)

Traditionally, the ITU-T and the IETF have proposed different methods of encoding the information that travels between endpoints.

It is generally accepted that applications using text-based encoding are easier to encode, decode, and troubleshoot, compared to Abstract Syntax Notation One (ASN.1)-based encoding, which is more compact and efficient.

Supplementary Services (Endpoint vs. Call Control)

Where and how you introduce supplementary services can be important considerations in a comparison of H.323, SIP, or MGCP.

Services deployed throughout the network are easily implemented centrally in a call control component. Services with regional relevance can be implemented effectively in the endpoints.

Strengths of H.323, SIP, and MGCP

Because there are several different telecommunication environments, more than one choice for signaling and call control is necessary. This topic looks at the strengths of H.323, SIP, and MGCP, and suggests the type of environment that best suits each call control model.

Strengths of H.323, SIP, and MGCP

- **H.323**
 - **Mature, stable, scalable**
 - **Large enterprise solution**
- **SIP**
 - **Dynamic, scalable, adaptable**
 - **Dynamic organization solution**
- **MGCP**
 - **Centralized management and control, scalable**
 - **Service provider solution**

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-3.5

H.323

H.323, which has been the only viable option in Voice over IP (VoIP) signaling and call control solutions for a long period of time, is mature and attracts supporters. Consequently, H.323 products are widely available and deployed extensively.

When properly designed, H.323 is both scalable (accommodates the implementation of large distributed networks) and adaptable (allows for the introduction of new features). The H.323 call control model works well for large enterprises because the gatekeeper-centralized call control provides some capability for Operation, Administration, and Maintenance (OA&M).

Session Initiation Protocol

SIP is a multimedia protocol that uses the architecture and messages that are found in popular Internet applications. By using a distributed architecture—with URLs for naming and text-based messaging—SIP takes advantage of the Internet model for building VoIP networks and applications.

SIP is a protocol that is used in a distributed architecture and allows companies to build large-scale networks that are scalable, resilient, and redundant. SIP provides mechanisms for interconnecting with other VoIP networks, and for adding intelligence and new features on the endpoints, SIP proxy, or redirect servers.

Although the IETF is progressive in defining extensions that allow SIP to work with legacy voice networks, the primary motivation behind SIP is to create an environment that supports next-generation communication models that utilize the Internet and Internet applications. In addition, the lack of centralized management support makes SIP more suitable for growing, dynamic organizations and Internet telephony service providers.

Media Gateway Control Protocol

MGCP describes an architecture in which call control and services such as OA&M are centrally added to a VoIP network. As a result, MGCP architecture closely resembles the existing public switched telephone network (PSTN) architecture and services.

In a centralized architecture, MGCP allows companies to build large-scale networks that are scalable, resilient, and redundant. MGCP provides mechanisms for interconnecting with other VoIP networks and adding intelligence and features to the call agent.

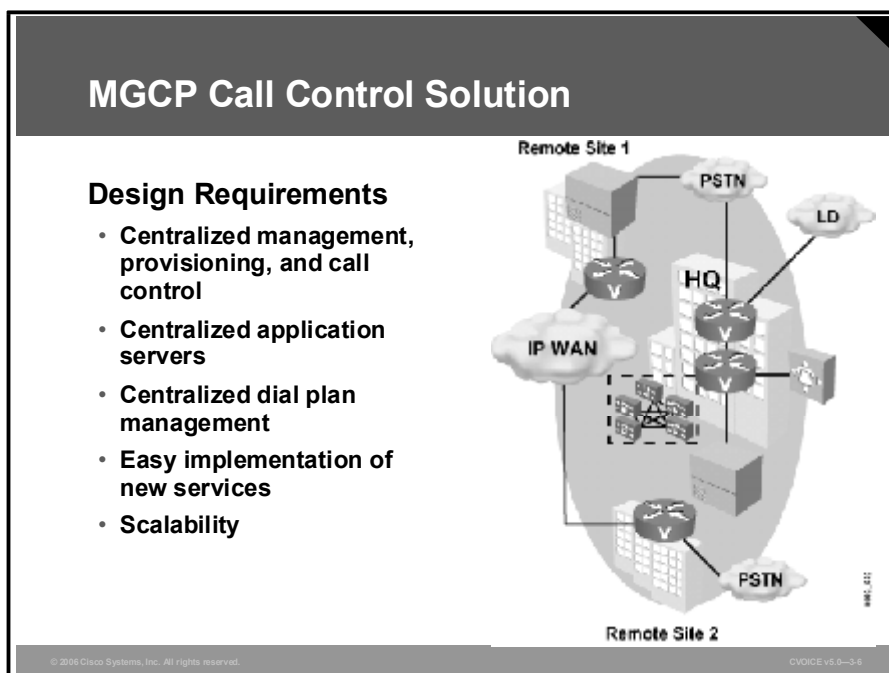
MGCP works well for organizations that are comfortable with centralized management and control; for example, service providers are well suited for MGCP.

Selecting Appropriate Call Control

Call control selection takes into account corporate policy and business requirements. This topic looks at different requirement scenarios and discusses which call control model best addresses those requirements.

MGCP Call Control Model

The MGCP call control model is used when there is a strong requirement for centralized control.

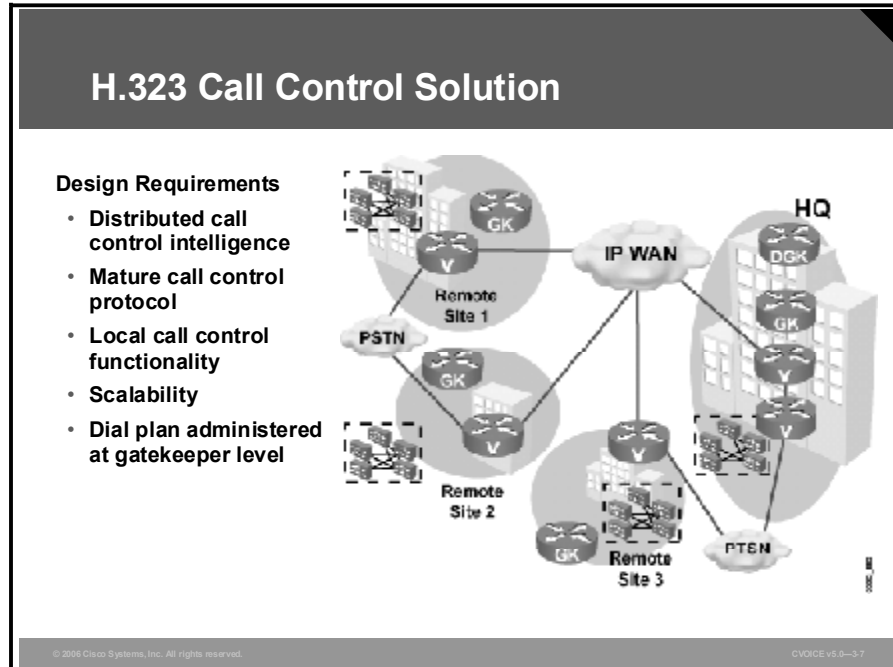


The MGCP call control model supports these design requirements:

- **Centralized management, provisioning, and call control:** All intelligence resides in the MGCP call agent. This approach presents a central site for configuration management, provisioning of new devices and endpoints, and call control configuration.
- **Centralized application servers:** Although centralized application servers are not required in an MGCP environment, typically when there is a strong requirement to centralize call control, the same requirement is applied to application servers.
- **Centralized dial plan management:** MGCP enables a centralized approach to dial plan management. All configurations for access to endpoints reside in the central call agent.
- **Easy implementation of new services:** When new services are implemented in a centralized call control model, only the call agent needs to be updated. Individual gateways across the enterprise can remain untouched, speeding the implementation of upgrades and new services and simplifying fallback procedures.
- **Scalability:** Cisco CallManager clusters acting as MGCP call agents can support up to 10,000 devices per cluster.

The H.323 Call Control Model

The H.323 call control model is used when there is a strong requirement for mature standards with distributed call logic functionality.

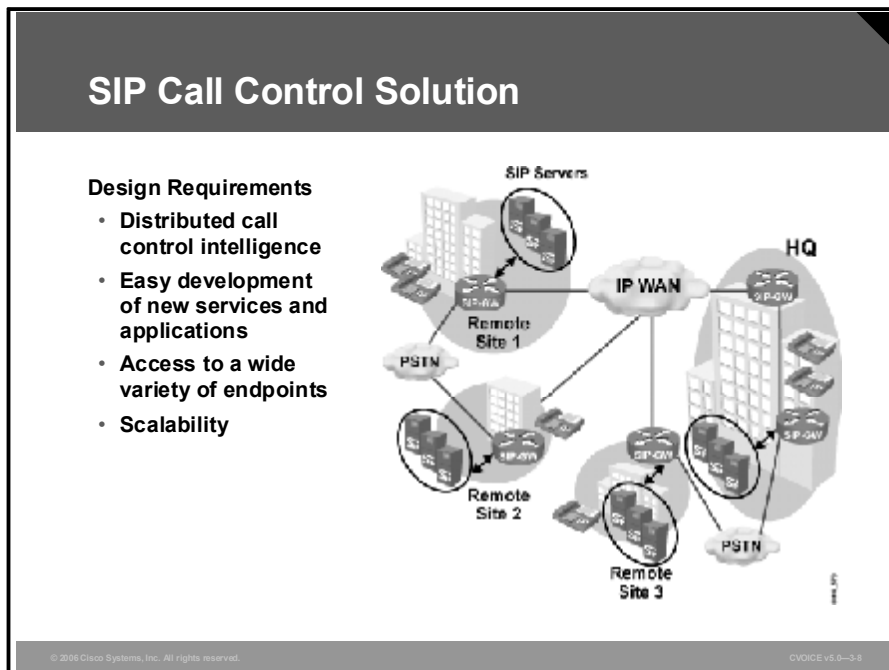


The H.323 call control model supports these design requirements:

- **Distributed call control intelligence:** H.323 gateways contain the intelligence to perform all required functions for call routing, call completion, and call termination. External call control servers are not required.
- **Mature call control protocol:** H.323 was designed for multimedia transport across a LAN environment. It was first approved in 1996. H.323 is widely deployed because it was the first comprehensive voice-signaling protocol available for VoIP deployment.
- **Local call control functionality:** The ability to add applications locally allows individual sites to implement and control applications independently of the head office. This ability enables locations to quickly implement new services when they are required.
- **Scalability:** As H.323 networks grow, gatekeepers provide scalability by dividing the growing network into zones and distributing controlling call configuration to a gatekeeper per zone. When the number of zones grows, hierarchical scalability provides for the use of directory gatekeepers to provide summarization for multiple zone gatekeepers.
- **Dial plan administered at gatekeeper level:** When the VoIP network expands, configuring dial plans in individual gateways becomes cumbersome and inefficient. H.323 specifies the ability for a gatekeeper to dynamically learn dial plan assignments from gateways, thereby simplifying dial plan configuration in large networks.

SIP Call Control Model

The SIP call control model is used when there is a strong requirement for innovative services and application deployment with distributed call logic functionality.



The SIP call control model supports these design requirements:

- **Distributed call control intelligence:** SIP gateways contain the intelligence to perform all required functions for call routing, call completion, and call termination. External call control servers are not required.
- **Easy development of new services and applications:** The use of widely deployed Internet standards such as HTTP and Simple Mail Transfer Protocol (SMTP) as part of the SIP standard translates into a large base of developers with the ability to create SIP-enabled applications.
- **Access to a wide variety of endpoints:** SIP-enabled endpoints include IP Phones, PCs, laptops, personal digital assistants (PDAs), and cell phones.
- **Scalability:** SIP operates in a stateless manner so that servers do not need to maintain state information and can handle more concurrent sessions. The use of proxy servers, redirect servers, location servers, and registrar servers enables large groups of users to communicate efficiently.

Summary

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

Summary

- **H.323, SIP, and MGCP provide signaling and call control, each in their own way.**
- **H.323 suits large enterprises; SIP suits small organizations; MGCP suits service providers.**
- **MGCP is suitable where centralized call control is required.**
- **H.323 is suitable where a mature standard and distributed call control is required.**
- **SIP is suitable where development and deployment of new services and applications in a distributed call control environment is required.**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0-3-8

References

For additional information, refer to these resources:

- ITU-T Recommendation H.323 (version 4).
<http://www.itu.int/rec/recommendation.asp?type=items&lang=E&parent=T-REC-H.323-200011-S>.
- IETF RFC 3261, *SIP: Session Initiation Protocol*.
<http://www.faqs.org/rfcs/rfc3261.html>.
- IETF RFC 2705, *Media Gateway Control Protocol (MGCP) Version 1.0*.
<http://www.faqs.org/rfcs/rfc2705.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) The encoding of which call control model is more compact but harder to decode and troubleshoot?

- A) H.323
- B) SGCP
- C) SIP
- D) MGCP

Q2) Match the type of endpoint to its call control model. An endpoint can be used more than once.

- A) client
- B) terminal
- C) gateway
- D) media gateway

_____ 1. H.323

_____ 2. SIP

_____ 3. MGCP

Q3) Match the common control component with the call control model. A common control component may be used more than once.

- A) call agent
- B) gatekeeper
- C) proxy server
- D) redirect server
- E) location server
- F) registrar server

_____ 1. MGCP

_____ 2. SIP

_____ 3. H.323

Q4) Match the signaling transport method with the call control model.

- A) UDP
- B) TCP
- C) UDP and TCP
- D) UDP or TCP

_____ 1. H.323

_____ 2. SIP

_____ 3. MGCP

- Q5) Which two components are responsible for address management in the SIP call control model? (Choose two.)
- A) proxy server
 - B) location server
 - C) registrar server
 - D) redirect server
- Q6) Match the method of supplemental service control with the call control model.
- A) provided by endpoints or call control
 - B) provided by endpoints
 - C) provided by call control
- _____ 1. H.323
- _____ 2. SIP
- _____ 3. MGCP
- Q7) Which call control model most closely resembles the PSTN?
- A) H.323
 - B) SGCP
 - C) SIP
 - D) MGCP
- Q8) Which call control model is popular in large enterprises because of its maturity and stability?
- A) H.323
 - B) SGCP
 - C) SIP
 - D) MGCP
- Q9) Which two call control models are suitable in a distributed call control architecture? (Choose two.)
- A) H.323
 - B) MGCP
 - C) Megaco
 - D) SIP
 - E) H.248
- Q10) Which call control model is based on HTTP and SMTP, and enables easy development of new services and applications?
- A) SIP
 - B) MGCP
 - C) H.323
 - D) H.248
- Q11) MGCP supports which of these requirements?
- A) integration with instant messaging
 - B) distributed call processing
 - C) scalability through the use of proxy servers, redirect servers, registrar servers, and location servers.
 - D) call processing controlled from a central server with no intelligence at the endpoints

Lesson Self-Check Answer Key

- Q1) A
Relates to: Feature Comparison Charts
- Q2) 1-C or B
2-A
3-C or D
Relates to: Feature Comparison Charts
- Q3) 1-A
2-C, D, E, or F
3-A and B
Relates to: Feature Comparison Charts
- Q4) 1-C
2-D
3-A
Relates to: Feature Comparison Charts
- Q5) B, C
Relates to: Feature Comparison Charts
- Q6) 1-A
2-A
3-C
Relates to: Feature Comparison Charts
- Q7) D
Relates to: Strengths of H.323, SIP, and MGCP
- Q8) A
Relates to: Strengths of H.323, SIP, and MGCP
- Q9) A, D
Relates to: Selecting Appropriate Call Control
- Q10) A
Relates to: Selecting Appropriate Call Control
- Q11) D
Relates to: Selecting Appropriate Call Control

Module 4

Improving and Maintaining Voice Quality

Overview

When human speech is converted to analog electrical signals and then digitized and compressed, some of the qualitative components are lost. This module explores the components of voice quality that you must maintain, the methods that you can use to measure voice quality, and the effective quality of service (QoS) tools that you can implement in a network to improve voice quality.

Module Objectives

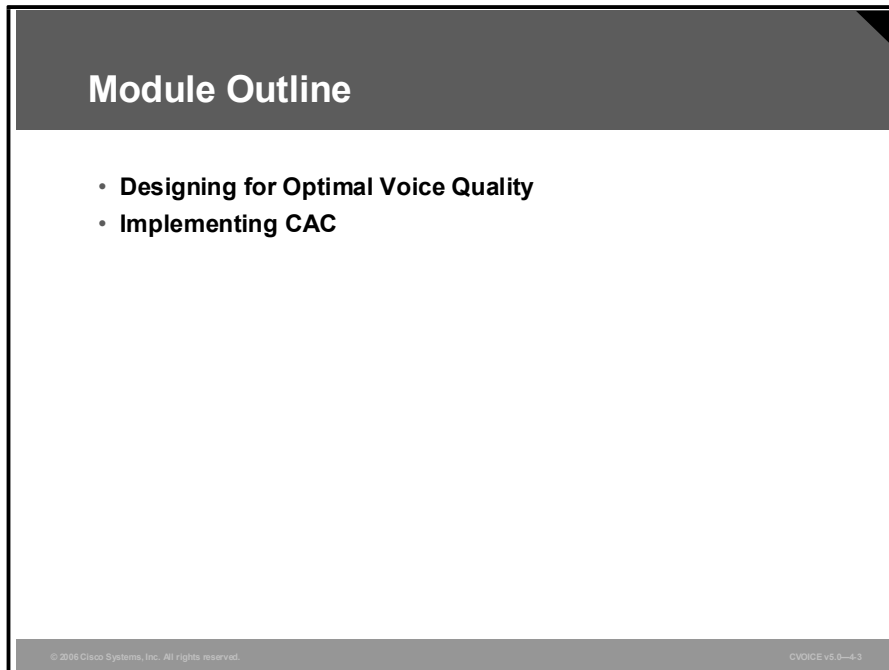
Upon completing this module, you will be able to describe specific voice quality issues and the QoS solutions used to solve them.

Module Objectives

- **Identify the problems presented by IP networks that affect voice and describe the QoS mechanisms used to address those problems**
- **Configure call control on the network using CAC tools and mechanisms**

Module Outline

The outline lists the components of this module.



Module Outline

- **Designing for Optimal Voice Quality**
- **Implementing CAC**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-6.3

Lesson 1

Designing for Optimal Voice Quality

Overview

Because of the inherent characteristics of a converged voice and data IP network, administrators face certain challenges in delivering voice traffic correctly. This lesson describes these challenges and offers solutions for avoiding and overcoming them when designing for optimal voice quality.

Objectives

Upon completing this lesson, you will be able to implement a converged voice and data IP network with optimal voice quality. This ability includes being able to meet these objectives:

- List the problems related to providing audio clarity in IP networks
- Describe techniques for minimizing jitter in an IP network
- Describe the factors to be considered when calculating the fixed and variable delay components of delay budget
- State the levels of delay defined as acceptable by the G.114 standard
- Describe how the Cisco VoIP solution mitigates packet loss in an IP network
- Explain why PESQ is a better measurement of voice quality in VoIP networks than MOS or PSQM
- Explain each of the objectives of QoS with an example
- Describe the features of Cisco IOS software that deliver QoS throughout the network
- Illustrate the characteristics of a poorly designed network with examples
- Describe how Cisco AutoQoS helps customers quickly deploy IP QoS and IP services

Outline

The outline lists the topics included in this lesson.

Outline

- **Overview**
- **IP Networking Overview**
- **Jitter**
- **Delay**
- **Acceptable Delay**
- **Packet Loss**
- **PESQ, MOS, and PSQM**
- **Objectives of QoS**
- **Using QoS to Improve Voice Quality**
- **Recognizing Common Design Faults**
- **Cisco AutoQoS Features**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0-6.2

IP Networking Overview

This topic describes the factors present in IP networks that affect audio clarity.

Factors Affecting Audio Clarity

- **Fidelity**
- **Echo**
- **Jitter**
- **Delay**
- **Sidetone**
- **Background noise**

© 2006 Cisco Systems, Inc. All rights reserved. VOICE v5.0-4.3

Because of the nature of IP networking, voice packets sent via IP are subject to certain transmission problems. Conditions present in the network may introduce problems such as echo, jitter, or delay. These problems must be addressed with quality of service (QoS) mechanisms.

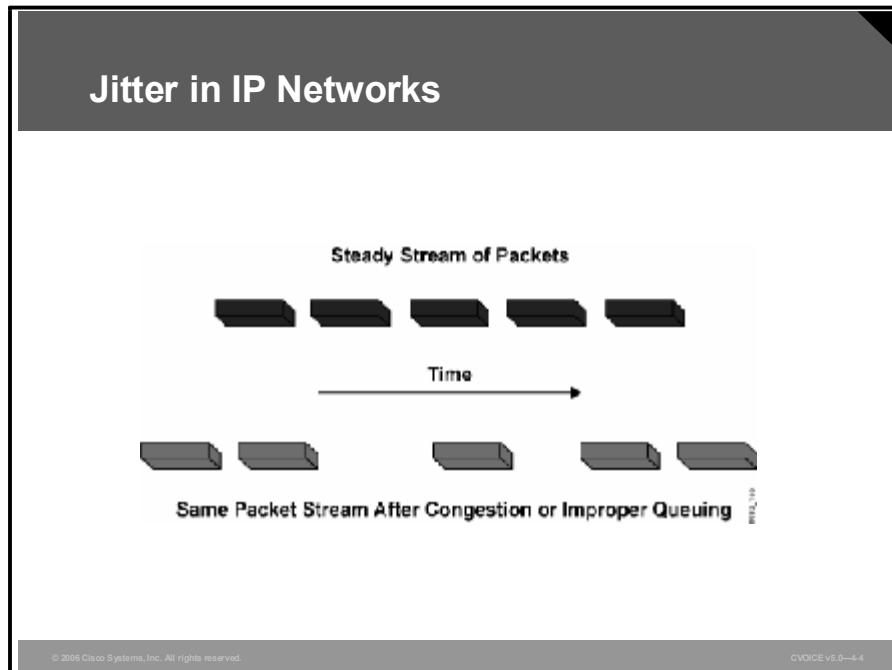
The clarity (or cleanliness and crispness) of the audio signal is of utmost importance. The listener must be able to recognize the identity and sense the mood of the speaker. These factors can affect clarity:

- **Fidelity:** Fidelity is the degree to which a system, or a portion of a system, accurately reproduces, at its output, the essential characteristics of the signal impressed upon its input or the result of a prescribed operation on the signal impressed upon its input (definition from the Alliance for Telecommunications Industry Solutions [ATIS]). The bandwidth of the transmission medium almost always limits the total bandwidth of the spoken voice. Human speech typically requires a bandwidth from 100 to 10,000 Hz, although 90 percent of speech intelligence is contained between 100 and 3000 Hz.
- **Echo:** Echo is a result of electrical impedance mismatches in the transmission path. Echo is always present, even in traditional telephony networks, but at a level that cannot be detected by the human ear. The two components that affect echo are amplitude (loudness of the echo) and delay (the time between the spoken voice and the echoed sound). You can control echo using suppressors or cancellers.
- **Jitter:** Jitter is variation in the arrival of coded speech packets at the far end of a Voice over IP (VoIP) network. The varying arrival time of the packets can cause gaps in the re-creation and playback of the voice signal. These gaps are undesirable and annoy the listener. Delay is induced in the network by variation in the routes of individual packets, contention, or congestion. You can resolve variable delay by using dejitter buffers.

- **Delay:** Delay is the time between the spoken voice and the arrival of the electronically delivered voice at the far end. Delay results from multiple factors, including distance (propagation delay), coding, compression, serialization, and buffers.
- **Sidetone:** Sidetone is the purposeful design of the telephone that allows the speaker to hear the spoken audio in the earpiece. Without sidetone, the speaker is left with the impression that the telephone instrument is not working.
- **Background noise:** Background noise is the low-volume audio that is heard from the far-end connection. Certain bandwidth-saving technologies can eliminate background noise altogether, such as voice activity detection (VAD). When this technology is implemented, the speaker audio path is open to the listener, while the listener audio path is closed to the speaker. The effect of VAD is often that speakers think that the connection is broken because they hear nothing from the other end.

Jitter

This topic describes the occurrence of jitter in IP networks and the Cisco solution to this problem.



Jitter is defined as a variation in the delay of received packets. On the sending side, packets are sent in a continuous stream with the packets spaced evenly. Because of network congestion, improper queuing, or configuration errors, this steady stream can become uneven because the delay between each packet varies instead of remaining constant, as displayed in the figure.

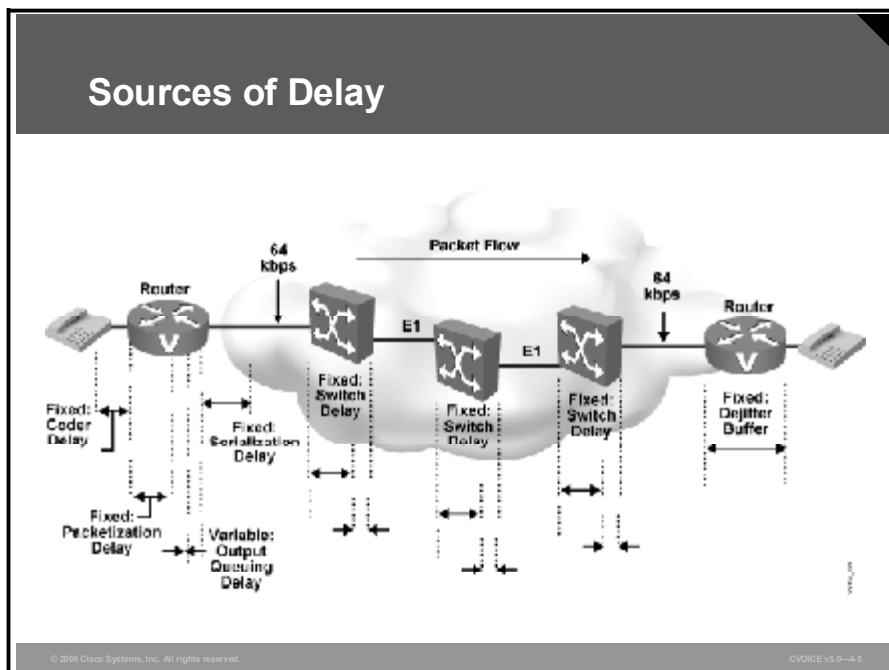
When a router receives an audio stream for VoIP, it must compensate for the jitter that is encountered. The mechanism that handles this function is the playout delay buffer, or dejitter buffer. The playout delay buffer must buffer these packets and then play them out in a steady stream to the digital signal processors (DSPs) to be converted back to an analog audio stream. The playout delay buffer, however, affects overall absolute delay.

Example: Jitter in Voice Networks

When a conversation is subjected to jitter, the results can be clearly heard. If the talker says, "Watson, come here. I want you," the listener might hear, "Wat...s...on.....come here, I.....wa.....nt.....y.....ou." The variable arrival of the packets at the receiving end causes the speech to be delayed and garbled.

Delay

Overall or absolute delay can affect VoIP. You may have experienced delay in a telephone conversation with someone on a different continent. The delays can cause entire words in the conversation to be cut off, and can therefore be very frustrating. This topic describes the causes of packet delay and the Cisco solution to this problem.



When you design a network that transports voice over packet, frame, or cell infrastructures, it is important to understand and account for the predictable delay components in the network. You must also correctly account for all potential delays to ensure that overall network performance is acceptable. Overall voice quality is a function of many factors, including the compression algorithm, errors and frame loss, echo cancellation, and delay.

Here are the two distinct types of delay:

- **Fixed delay:** Fixed-delay components are predictable and add directly to overall delay on the connection. Fixed-delay components include those listed here:
 - **Coding:** The time that it takes to translate the audio signal into a digital signal
 - **Packetization:** The time that it takes to put digital voice information into packets and remove the information from packets
 - **Serialization:** The insertion of bits onto a link
 - **Propagation:** The time that it takes a packet to traverse a link
- **Variable delays:** Variable delays arise from queuing delays in the egress trunk buffers that are located on the serial port that is connected to the WAN. These buffers create variable delays, called jitter, across the network.

Acceptable Delay

This topic describes the level of delay defined as acceptable by the G.114 standard.

Range in Milliseconds	Description
0 to 150	Acceptable for most user applications
150 to 400	Acceptable, provided that administrators are aware of the transmission time and its impact on the transmission quality of user applications
Above 400	Unacceptable for general network planning purposes (However, it is recognized that in some exceptional cases, this limit will be exceeded.)

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) specifies network delay for voice applications in Recommendation G.114. This recommendation defines three bands of one-way delay, as shown in the table in the figure.

Note This recommendation is for connections with echo that are adequately controlled, implying that echo cancellers are used. Echo cancellers are required when one-way delay exceeds 25 ms (G.131).

This recommendation is oriented toward national telecommunications administrations and, therefore, is more stringent than recommendations that would normally be applied in private voice networks. When the location and business needs of end users are well known to a network designer, more delay may prove acceptable. For private networks, a 200-ms delay is a reasonable goal and a 250-ms delay is a limit. This goal is what Cisco Systems proposes as reasonable as long as excessive jitter does not affect voice quality. However, all networks must be engineered so that the maximum expected voice connection delay is known and minimized.

Example: Acceptable Delay

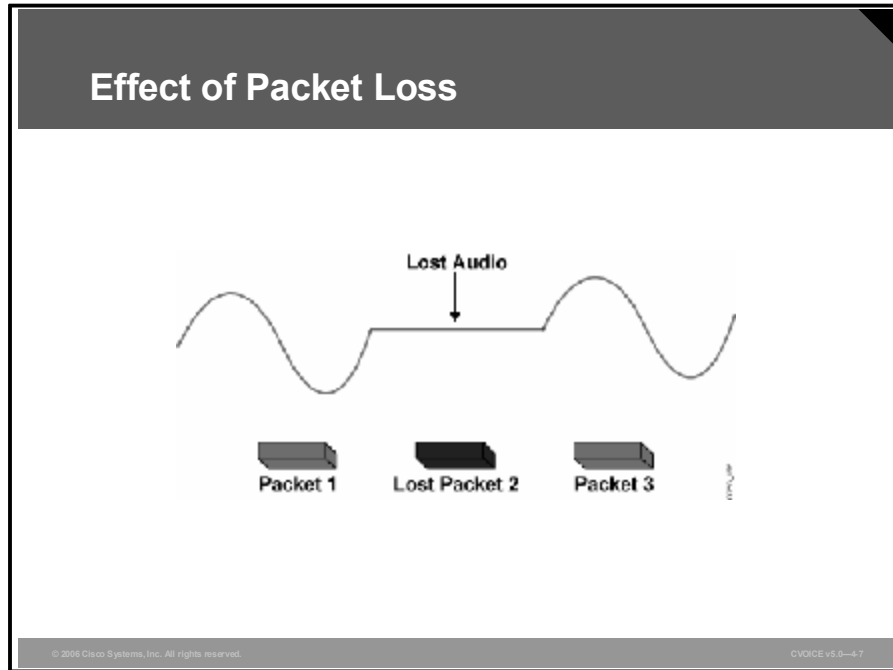
The G.114 recommendation is for one-way delay only and does not account for round-trip delay. Network design engineers must consider both variable and fixed delays. Variable delays include queuing and network delays, while fixed delays include coding, packetization, serialization, and dejitter buffer delays. The table is an example of calculating delay budget.

Calculating Delay Budget

Delay Type	Fixed (ms)	Variable (ms)
Coder delay	18	
Packetization delay	30	
Queuing and buffering		8
Serialization (64 kbps)	5	
Network delay (public frame)	40	25
Dejitter buffer	45	
Totals	138	33

Packet Loss

Lost data packets are recoverable if the endpoints can request retransmission. Lost voice packets are *not* recoverable, because the audio must be played out in real time and retransmission is not an option. This topic describes the causes and effects of lost voice packets.



Voice packets may be dropped under these conditions:

- The network is unstable (flapping links).
- The network is congested.
- There is too much variable delay in the network.

Packet loss causes voice clipping and skips. As a result, the listener hears gaps in the conversation, as shown in the figure. The industry standard coder-decoder (codec) algorithms that are used in Cisco DSPs will correct for 20 ms to 50 ms of lost voice through the use of Packet Loss Concealment (PLC) algorithms. PLC intelligently analyzes missing packets and generates a reasonable replacement packet to improve the voice quality. Cisco VoIP technology uses 20-ms samples of voice payload per VoIP packet by default. Effective codec correction algorithms require that only a single packet can be lost at any given time. If more packets are lost, the listener experiences gaps.

Example: Packet Loss in Voice Networks

If a conversation experiences packet loss, the effect is immediately heard. If the talker says, “Watson, come here. I want you,” the listener might hear, “Wat----, come here, -----you.”

PESQ, MOS, and PSQM

This topic explains mean opinion score (MOS), Perceptual Speech Quality Measurement (PSQM), and Perceptual Evaluation of Speech Quality (PESQ). It also compares the functionality of these measurement standards.

MOS and PSQM

MOS

- Acronym for mean opinion score
- Defined in ITU-T Recommendation P.800
- Results in subjective measures
- Scores from 1 (worst) to 5 (best); 4.0 is toll quality

PSQM

- Acronym for Perceptual Speech Quality Measurement
- Defined in ITU Standard P.861
- Automated in-service measurement
- Scores from 6.5 (worst) to 0 (best)

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-4.8

Mean Opinion Score

MOS is a scoring system for voice quality. A MOS score is generated when listeners evaluate prerecorded sentences that are subject to varying conditions, such as compression algorithms. Listeners then assign the sentences values, based on a scale from 1 to 5, where 1 is the worst and 5 is the best. The sentence used for English-language MOS testing is, “Nowadays, a chicken leg is a rare dish.” This sentence is used because it contains a wide range of sounds found in human speech, such as long vowels, short vowels, hard sounds, and soft sounds.

The test scores are then averaged to a composite score. The test results are subjective, because they are based on the opinions of the listeners. The tests are also relative, because a score of 3.8 from one test cannot be directly compared to a score of 3.8 from another test. Therefore, you must establish a baseline for all tests, such as G.711, so that the scores can be normalized and compared directly.

Perceptual Speech Quality Measurement

PSQM is an automated method of measuring speech quality “in service,” or as the speech happens. PSQM software usually resides with IP call management systems, which are sometimes integrated into Simple Network Management Protocol (SNMP) systems.

Equipment and software that can measure PSQM is available through third-party vendors; it is not implemented in Cisco equipment. The measurement is made by comparing the original transmitted speech to the resulting speech at the far end of the transmission channel. PSQM systems are deployed as in-service components. The PSQM measurements are made during real conversation on the network. This automated testing algorithm has over 90 percent accuracy compared to subjective listening tests, such as MOS. Scoring is based on a scale from 0 to 6.5, where 0 is the best and 6.5 is the worst. Because it was originally designed for circuit-switched voice, PSQM does not take into account the jitter or delay problems that are experienced in packet-switched voice systems.

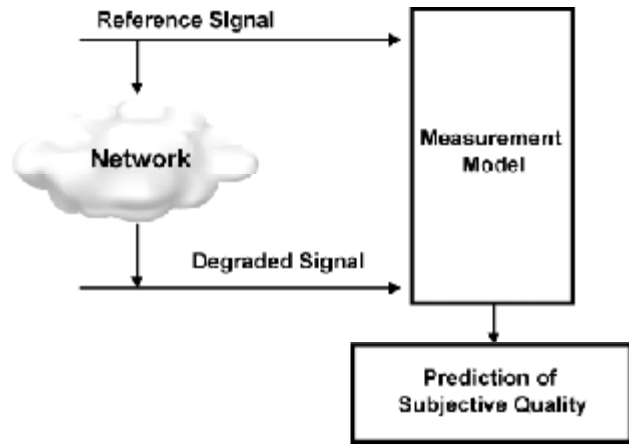
Example: MOS and PSQM in VoIP Networks

MOS and PSQM are not recommended for present-day VoIP networks. Both were originally designed before the emergence of VoIP technologies and do not measure typical VoIP problems such as jitter and delay. For example, it is possible to obtain an MOS score of 3.8 on a VoIP network when the one-way delay exceeds 500 ms. This is because the MOS evaluator has no concept of a two-way conversation and listens only to audio quality. The one-way delay is not evaluated.

Perceptual Evaluation of Speech Quality

PESQ was originally developed by British Telecommunications, Psytechnics, and KPN Research in the Netherlands. It has evolved into ITU-T Recommendation P.862, which is considered the current standard for voice quality measurement. PESQ can take into account codec errors, filtering errors, jitter problems, and delay problems that are typical in a VoIP network. It combines the best of the PSQM method along with a method called Perceptual Analysis Measurement System (PAMS). PESQ scores range from 1 (worst) to 4.5 (best), with 3.8 considered toll quality (acceptable quality in a traditional telephony network). PESQ is meant to measure only one aspect of voice quality. The effects of two-way communication, such as loudness loss, delay, echo, and sidetone, are not reflected in PESQ scores.

Perceptual Evaluation of Speech Quality



© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0-6.0

Example: PESQ Applied

Many equipment vendors offer PESQ measurement systems. Such systems are either standalone or plug into existing network management systems. PESQ was designed to mirror the MOS measurement system; therefore, if a score of 3.2 is measured by PESQ, a score of 3.2 should be achieved using MOS methods.

Quality Measurement Comparison

Early quality measurement methods, such as MOS and PSQM, were designed before widespread acceptance of VoIP technology. PESQ was designed to address the shortcomings of MOS and PSQM.

Voice Quality Measurement Comparison

Feature	MOS	PSQM	PESQ
Test method	Subjective	Objective	Objective
End-to-end packet loss test	Inconsistent	No	Yes
End-to-end jitter test	Inconsistent	No	Yes

© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-4-10

MOS uses subjective testing in which the average opinion of a group of test users is calculated to create the MOS score. This method is both time-consuming and expensive and may not provide consistent results between groups of testers.

PSQM and PESQ use objective testing in which an original reference file sent into the system is compared with the impaired signal that came out. This testing method provides an automated test mechanism that does not rely on human interpretation for result calculations. However, PSQM was originally designed for circuit-switched networks and does not take into account the effects of jitter and packet loss.

PESQ measures the effect of end-to-end network conditions, including codec processing, jitter, and packet loss. PESQ is the preferred method of testing voice quality in an IP network.

Objectives of QoS

To ensure that VoIP is an acceptable replacement for standard public switched telephone network (PSTN) telephony services, customers must receive the same consistently high quality of voice transmission that they receive with basic telephone services. This topic discusses how QoS can help you achieve this objective.

Objectives of QoS

QoS has these objectives:

- **Supporting dedicated bandwidth**
- **Improving loss characteristics**
- **Avoiding and managing network congestion**
- **Shaping network traffic**
- **Setting traffic priorities across the network**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-4-11

Like other real-time applications, VoIP is extremely sensitive to issues related to bandwidth and delay. To ensure that VoIP transmissions are intelligible to the receiver, voice packets cannot be dropped, excessively delayed, or subject to variations in delay (jitter).

Example: QoS Objectives

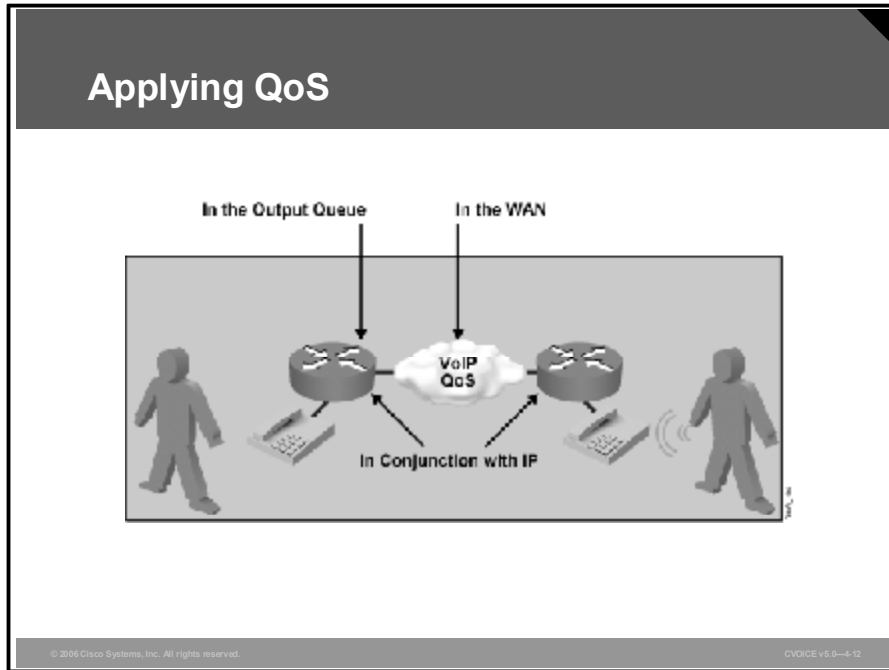
VoIP guarantees high-quality voice transmission only if the signaling and audio channel packets have priority over other kinds of network traffic. A successful VoIP deployment must provide an acceptable level of voice quality by meeting VoIP traffic requirements for issues related to bandwidth, latency, and jitter. QoS provides better, more predictable network service by meeting these objectives:

- **Supporting dedicated bandwidth:** Designing the network such that the necessary bandwidth is always available to support voice and data traffic
- **Improving loss characteristics:** Designing the Frame Relay network such that discard eligibility is not a factor for frames containing voice, keeping voice below the committed information rate (CIR)
- **Avoiding and managing network congestion:** Ensuring that the LAN and WAN infrastructure can support the volume of data traffic and voice calls

- **Shaping network traffic:** Using Cisco traffic-shaping tools to ensure smooth and consistent delivery of frames to the WAN
- **Setting traffic priorities across the network:** Marking the voice traffic as priority and queuing it first

Using QoS to Improve Voice Quality

Voice features that provide QoS are deployed at different points in the network and designed for use with other QoS features to achieve specific goals, such as minimization of jitter and delay. This topic identifies the network areas in which QoS is implemented in Cisco networks.



Cisco IOS software includes a complete set of features for delivering QoS throughout the network. This list presents the Cisco IOS features that address the voice packet delivery requirements of end-to-end QoS and service differentiation.

- In the output queue of the router:
 - **Class-based weighted fair queuing (CBWFQ):** CBWFQ extends the standard weighted fair queuing (WFQ) functionality by providing support for user-defined traffic classes. You can create a specific class for voice traffic by using CBWFQ.
 - **Low Latency Queuing (LLQ):** LLQ provides strict priority queuing (PQ) in conjunction with CBWFQ. LLQ configures the priority status for a class within CBWFQ in which voice packets receive priority over all other traffic. LLQ is considered a best practice by the Cisco Enterprise Solutions Engineering (ESE) group for delivering voice QoS services over a WAN.
 - **WFQ:** WFQ segregates traffic into flows and then schedules traffic onto the outputs to meet specified bandwidth allocation or delay bounds.
 - **Weighted random early detection (WRED):** WRED provides differentiated performance characteristics for different classes of service. This classification allows preferential handling of voice traffic under congestion conditions without worsening the congestion.

- In the WAN or WAN protocol:
 - **Committed access rate (CAR):** CAR provides a rate-limiting feature for allocating bandwidth commitments and bandwidth limitations to traffic sources and destinations. At the same time, CAR specifies policies for handling the traffic that may exceed bandwidth allocation.
 - **Frame Relay traffic shaping (FRTS):** FRTS delays excess traffic by using a buffer or queuing mechanism to hold packets and shape the flow when the data rate of the source is higher than expected.
 - **Frame Relay Forum Standard 12 (FRF.12):** FRF.12 ensures predictability for voice traffic by providing better throughput on low-speed Frame Relay links. FRF.12 interleaves delay-sensitive voice traffic on one virtual circuit (VC) with fragments of a long frame on another VC that is using the same interface.
 - **IP to ATM class of service (CoS):** IP to ATM CoS includes a feature suite that maps CoS characteristics between the IP and ATM. It also offers differentiated service classes across the entire WAN—not just the routed portion—and gives mission-critical applications exceptional service during periods of high network usage and congestion.
 - **Multilink PPP (MLP) with link fragmentation and interleaving (LFI):** MLP with LFI allows large packets to be multilink-encapsulated and fragmented so that they are small enough to satisfy the delay requirements of real-time traffic. MLP with LFI also provides a special transmit queue for smaller, delay-sensitive packets, enabling them to be sent earlier than other flows.
- In conjunction with the operation of IP:
 - **Compressed Real-Time Transport Protocol (CRTP):** The Real-Time Protocol (RTP) is a protocol for the transport of real-time data, including voice. RTP uses extensive headers that incorporate time stamps for individual packets. CRTP compresses the extensive RTP header when used in conjunction with RTP. The result is decreased consumption of available bandwidth for voice traffic and a corresponding reduction in delay.
 - **Resource Reservation Protocol (RSVP):** RSVP supports the reservation of resources across an IP network, allowing end systems to request QoS guarantees from the network. For networks that support VoIP, RSVP—in conjunction with features that provide queuing, traffic shaping, and voice call signaling—provides Call Admission Control (CAC) for voice traffic.
 - **QoS policy propagation on Border Gateway Protocol (BGP):** This feature prepares BGP to distribute QoS policy to remote routers in a network. It allows classification of packets and then uses other QoS features, such as CAR and WRED, to specify and enforce business policies to fit a business model.

Recognizing Common Design Faults

Successful implementations of delay-sensitive applications such as VoIP require a network that is carefully engineered with QoS from end to end. Fine-tuning the network to adequately support VoIP involves a series of protocols and features that are geared toward improving voice quality. This topic identifies the characteristics of a poorly designed network.

What Makes a Design Bad?

- Ignoring Layer 2 QoS requirements
- Ignoring other QoS requirements
- Ignoring bandwidth considerations
- Simply adding VoIP to an existing IP network

The diagram illustrates a network topology where a PBX is connected to a central router, which is connected to a VoIP cloud, and then to another central router connected to a PSTN. A question mark is placed below the VoIP cloud, indicating a design fault.

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-4-13

QoS is the ability of a network to provide better service levels to selected network traffic over various underlying technologies. QoS is not inherent in a network infrastructure. Instead, QoS is implemented by strategically enabling appropriate QoS features throughout the network.

Poor design is characterized by these issues:

- **Ignoring Layer 2 QoS requirements:** QoS technologies such as priority Layer 2 congestion management, FRF.12, LFI, and traffic shaping must be correctly configured.
- **Ignoring other QoS requirements:** QoS technologies such as LLQ, RTP, congestion management, and congestion avoidance must be enabled.
- **Ignoring bandwidth considerations:** Planning for the total number of calls and their effect on data bandwidth is critical to all users of the network.
- **Simply adding VoIP to an existing IP network:** When considering VoIP, network administrators must insist on a complete network redesign for a comprehensive end-to-end solution.

Example: Deploying QoS

Many people believe that the fastest way to fix network performance is to simply add a lot of bandwidth. That approach may work well in certain situations, such as campus networks, in which upgrading from 10-Mbps to 100-Mbps or even 1-GB links may be possible. But it is not always feasible to add bandwidth in a WAN. Upgrading a WAN circuit from 56 kbps to T1 may be cost prohibitive and may not be possible for certain locations on the network. To provide effective performance in a voice network, you must configure QoS throughout the network and not just on the Cisco devices that are running VoIP. Not all QoS techniques are appropriate for all network routers. Edge routers and backbone routers in a network do not necessarily perform the same operations; the QoS tasks that they perform may differ as well. To configure an IP network for real-time voice traffic, you must consider the functions of both edge and backbone routers and select the appropriate QoS tools.

Cisco AutoQoS Features

This topic describes Cisco AutoQoS features and the associated command structure for routers.

Cisco AutoQoS Features

Cisco AutoQoS addresses the five key elements of QoS deployment:

- **Application classification**
- **Policy generation**
- **Configuration**
- **Monitoring and reporting**
- **Consistency**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0—4-15

Cisco AutoQoS is an innovative technology that minimizes the complexity, time, and operating cost of QoS deployment. Cisco AutoQoS incorporates value-added intelligence into Cisco IOS software and Cisco Catalyst software to provision and manage large-scale QoS deployments.

To expedite QoS deployment, the user interface must be simplified. Cisco AutoQoS addresses this issue by automating these five main aspects of QoS deployment while adding control plane intelligence to create a simple, accelerated, and tunable solution:

- **Application classification:** Cisco AutoQoS identifies VoIP control and bearer traffic. Cisco AutoQoS uses Cisco Discovery Protocol for voice packets, ensuring that the device attached to the LAN is really an IP Phone.
- **Policy generation:** Cisco AutoQoS evaluates the network environment and automatically generates an initial policy on a given interface, port, or permanent virtual circuit (PVC).
- **Configuration:** With one command, Cisco AutoQoS configures the port to prioritize voice traffic without affecting other network traffic, while still offering the flexibility to adjust QoS settings for unique network environments. QoS settings are automatically disabled when a Cisco IP Phone is relocated or moved.
- **Monitoring and reporting:** Cisco AutoQoS provides visibility into the classes of service deployed via system logging and SNMP traps.
- **Consistency:** Cisco AutoQoS policies are designed to work in harmony with each other across Cisco devices, ensuring consistent end-to-end QoS.

The increased deployment of delay-sensitive applications (voice, video, and other multimedia applications) deployed in networks requires proper QoS configuration to ensure application performance.

Before the availability of Cisco AutoQoS, proper QoS configuration of a network required a deep understanding of various QoS features (that is, queuing, dropping, traffic conditioning, queue depth, drop thresholds, burst parameters, LFI, and RTP). The use of Cisco AutoQoS helps minimize the complexity of configuring a network correctly for QoS by automatically configuring the device with the correct QoS parameters. Cisco AutoQoS automates consistent deployment of QoS features across Cisco routers and switches. It enables various Cisco QoS components based on the network environment and Cisco best-practice recommendations.

Users can subsequently tune parameters that are generated by Cisco AutoQoS to suit their particular application needs.

Cisco AutoQoS performs these functions:

- On WAN interfaces:
 - Automatically classifies RTP payload and VoIP control packets (H.323, H.225 Unicast, Skinny Client Control Protocol [SCCP], session initiation protocol [SIP], Media Gateway Control Protocol [MGCP])
 - Builds service policies for VoIP traffic that are based on Cisco Modular QoS command-line interface (Modular QoS CLI)
 - Provisions LLQ PQ for VoIP bearer traffic and bandwidth guarantees for control traffic
 - Enables WAN traffic shaping that adheres to Cisco best practices, where required
 - Enables link efficiency mechanisms, such as LFI and RTP header compression (CRTP), where required
 - Provides SNMP and syslog alerts for VoIP packet drops
- On LAN interfaces:
 - Enforces the trust boundary on Cisco Catalyst switch access ports, uplinks, and downlinks
 - Enables Cisco Catalyst strict PQ (also known as expedite queuing) with weighted round-robin (WRR) scheduling for voice and data traffic, where appropriate
 - Configures queue admission criteria (maps CoS values in the incoming packets to the appropriate queues)
 - Modifies queue sizes and weights, where required

Note Cisco AutoQoS is available in the following Cisco IOS software releases: Cisco IOS Release 12.1E or later for the Cisco Catalyst 2950 Series switches and Cisco Catalyst 3550 Series switches; Cisco IOS Release 12.2T or later for the Cisco 2600 Series routers, Cisco 2600XM Series routers, Cisco 3600 Series routers, Cisco 3700 Series routers, and Cisco 7200 Series routers; Cisco IOS Release 12.1E or later for the Cisco Catalyst 4500 Series switches; and Cisco Catalyst software 7.5.1 or later for the Cisco Catalyst 6500 Series switches.

Typically, QoS network design and implementation over multiple LAN and WAN sites is fairly complex and labor-intensive. Customers wish to reduce deployment time, provisioning errors, and operating expenses to optimize their network for the applications while retaining the flexibility to subsequently fine-tune QoS.

Example: Span Engineering Implementation of Cisco AutoQoS

Span Engineering wishes to deploy QoS features to ensure optimal quality in its converged network. Currently, the company lacks the staff and expertise to design and implement IP QoS services. Span Engineering plans to utilize Cisco AutoQoS technology for initial deployment. The company plans to further fine-tune QoS parameters as it monitors the network and gains expertise in QoS configuration.

Configuring Cisco AutoQoS

```
interface Serial4/0
 encapsulation frame-relay
 frame-relay traffic-shaping
!
interface Serial4/0.0 point-to-point
 bandwidth 256
 ip address 10.1.71.1 255.255.255.0
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial4/0-100
  auto qos voip
 frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial4/0-100
 frame-relay cir 256000
 frame-relay bc 2560
 frame-relay be 0
 frame-relay mincir 256000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 320
```

West Coast

Dallas

Chicago

Frame Relay

Span Engineering Voice Network

FRTS enabled by AutoQoS (points to `frame-relay traffic-shaping`)

You specify bandwidth, IP address, and Frame Relay DLCI (points to `interface Serial4/0.0 point-to-point bandwidth 256 ip address 10.1.71.1 255.255.255.0 frame-relay interface-dlci 100`)

You enable AutoQoS (points to `class AutoQoS-VoIP-FR-Serial4/0-100 auto qos voip`)

CRTIP configuration generated by AutoQoS (points to `frame-relay ip rtp header-compression`)

FRTS and FRF.12 settings generated by AutoQoS (points to `map-class frame-relay AutoQoS-VoIP-FR-Serial4/0-100 frame-relay cir 256000 frame-relay bc 2560 frame-relay be 0 frame-relay mincir 256000`)

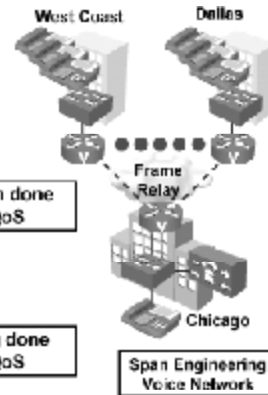
© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-4-15

Configuring Cisco AutoQoS (Cont.)

```
class-map match-any AutoQoS-VoIP-RTP-Untrust
  match protocol rtp audio
  match access-group name AutoQoS-VoIP-RTP
class-map AutoQoS-VoIP-Control-Untrust
  match access-group name AutoQoS-VoIP-Control
class-map match-any AutoQoS-VoIP-Remark
  match ip dscp ef
  match ip dscp af31
  !
policy-map AutoQoS-Policy-Untrust
  class-map AutoQoS-VoIP-RTP-Untrust
    priority percent 70
    set dscp ef
  class AutoQoS-VoIP-Control-Untrust
    bandwidth percent 5
    set dscp af31
  class AutoQoS-VoIP-Remark
    set dscp default
  class class-default
    fair-queue
```

Classification done by AutoQoS

Provisioning done by AutoQoS



© 2006 Cisco Systems, Inc. All rights reserved.

VOICE v5.0-4-16

In the example, Span Engineering completes the basic serial interface configuration that includes specifying the IP address and applying the required Frame Relay parameters. Cisco AutoQoS is enabled at the interface data-link connection identifier (DLCI) level with the command **auto qos voip**. The sample configuration shows the additional QoS parameters that were automatically generated by enabling Cisco AutoQoS.

Summary

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

Summary

- **The factors that affect audio clarity are fidelity, echo, delay, and jitter.**
- **Jitter is a variation in the delay of received packets.**
- **End-to-end network delay must be calculated to ensure acceptable quality voice .**
- **Recommendation G.114 defines maximum acceptable delay as 150 ms.**
- **Packet loss causes conversational gaps.**
- **MOS is a subjective method of measuring voice quality, using live testers to determine quality. PSQM is an objective, automated method of measuring voice quality, originally designed for circuit-switched networks. PESQ is an objective, automated method of measuring voice quality and is the preferred method in current VoIP implementations.**

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0—4-17

Summary (Cont.)

- **QoS supports dedicated bandwidth, improves loss characteristics, avoids and manages network congestion, shapes network traffic, and sets traffic priorities across the network.**
- **Cisco IOS software QoS for voice features can be implemented across the entire network.**
- **Ignoring Layer 2 and other QoS requirements and bandwidth considerations and simply adding VoIP to an existing IP network are poor network design elements that contribute to poor QoS.**
- **Cisco AutoQoS can be used to simplify the configuration of QoS.**

© 2006 Cisco Systems, Inc. All rights reserved.

CVOICE v5.0—4-18

References

For additional information, refer to these resources:

- PESQ information website.
<http://www.pesq.org>.
- *Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)*.
http://www.cisco.com/warp/public/788/voice-qos/jitter_packet_voice.html.
- *Understanding Delay in Packet Voice Networks*.
<http://www.cisco.com/warp/public/788/voip/delay-details.html>.
- Voice Quality.
http://www.cisco.com/en/US/tech/tk652/tk698/tsd_technology_support_protocol_home.html.
- Voice.
http://www.cisco.com/en/US/tech/tk652/tsd_technology_support_category_home.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) Which two factors affect voice clarity? (Choose two.)
- A) fidelity
 - B) echo
 - C) sidetone
 - D) background noise
 - E) distance
- Q2) Which two psychological comfort factors contribute to the quality of voice being perceived as good? (Choose two.)
- A) silence suppression
 - B) buffering
 - C) sidetone
 - D) background noise
 - E) ring cadence
- Q3) Which of these methods will most effectively reduce jitter in a VoIP network?
- A) by using dejitter buffers
 - B) by using FIFO queuing
 - C) by using header compression
 - D) by using guaranteed delay
- Q4) Variable delay is also known as _____.
- A) nondeterministic
 - B) jitter
 - C) playout delay
 - D) FIFO
- Q5) What are two categories of delay? (Choose two.)
- A) variable delay
 - B) serialization delay
 - C) fixed delay
 - D) FIFO delay
 - E) processing delay
- Q6) What is an example of variable delay?
- A) serialization delay
 - B) propagation delay
 - C) queuing delay
 - D) codec delay
- Q7) According to ITU-T Recommendation G.114 for national telecommunications administrations, how much delay is acceptable for most user applications?
- A) 0 ms to 150 ms
 - B) 200 ms to 250 ms
 - C) 150 ms to 400 ms
 - D) above 400 ms

- Q8) According to Cisco, what is the acceptable level of one-way delay for private networks?
- A) 0 ms to 150 ms
 - B) 200 ms to 250 ms
 - C) 150 ms to 400 ms
 - D) above 400 ms
- Q9) Which two conditions can result in voice packets being dropped? (Choose two.)
- A) slow links
 - B) too much noise
 - C) too much jitter
 - D) too much congestion
- Q10) In Cisco VoIP networks using default payload sizes, how many packets can be lost without the listener experiencing gaps in conversation?
- A) none
 - B) one
 - C) two
 - D) no more than five
- Q11) Which voice quality scoring system is based on subjective evaluation?
- A) MOS
 - B) PCM
 - C) PSQM
 - D) PESQ
- Q12) What is the accuracy of PSQM compared to other listening tests?
- A) over 50 percent
 - B) over 65 percent
 - C) over 90 percent
 - D) over 99.9 percent
- Q13) In PESQ measurements, which score is considered toll quality?
- A) 3.1
 - B) 3.8
 - C) 4.0
 - D) 6.5
- Q14) PESQ is defined as which ITU-T recommendation?
- A) P.800
 - B) P.861
 - C) P.862
 - D) G.711
- Q15) Why is VoIP highly sensitive to bandwidth and delay problems?
- A) because it transmits both voice and data
 - B) because it is a real-time application
 - C) because it is an older technology
 - D) because of its default settings

- Q16) Which is NOT an objective of QoS?
- A) improving loss characteristics
 - B) providing error correction
 - C) shaping network traffic
 - D) setting traffic priorities across the network
- Q17) Which two Cisco IOS software QoS features are employed in the output queue of the router? (Choose two.)
- A) FRF.12
 - B) IP to ATM CoS
 - C) CBWFQ
 - D) CRTP
 - E) RSVP
 - F) WRED
- Q18) Which two Cisco QoS features are deployed in the WAN? (Choose two.)
- A) CAR
 - B) DWFQ
 - C) MLP with LFI
 - D) QoS policy propagation via BGP
 - E) CRTP
- Q19) Which practice indicates a bad network design?
- A) completely redesigning the network
 - B) using LLQ
 - C) splitting and interleaving large data packets
 - D) ignoring bandwidth requirements
- Q20) Different QoS tools must be selected for each device based on _____.
- A) the devices that are running VoIP
 - B) the functions of the device
 - C) the country in which the device is located
 - D) the times of highest traffic
- Q21) Cisco AutoQoS automates consistent deployment of _____ features across Cisco routers and switches.
- A) fragmentation
 - B) traffic shaping
 - C) FRTS
 - D) QoS
- Q22) Cisco AutoQoS performs which three functions? (Choose three.)
- A) provides automatic configuration of bandwidth parameter on serial interfaces
 - B) builds service policies for VoIP traffic that are based on Cisco Modular QoS CLI
 - C) provisions LLQ PQ for VoIP bearer traffic and bandwidth guarantees for control traffic
 - D) enables WAN traffic shaping that adheres to Cisco best practices, where required
 - E) enables policing on WAN interfaces to reduce jitter and delay

Lesson Self-Check Answer Key

- Q1) A, B
Relates to: IP Networking Overview
- Q2) C, D
Relates to: IP Networking Overview
- Q3) A
Relates to: Jitter
- Q4) B
Relates to: Jitter
- Q5) A, C
Relates to: Delay
- Q6) C
Relates to: Delay
- Q7) A
Relates to: Acceptable Delay
- Q8) B
Relates to: Acceptable Delay
- Q9) C, D
Relates to: Packet Loss
- Q10) B
Relates to: Packet Loss
- Q11) A
Relates to: PESQ, MOS, and PSQM
- Q12) C
Relates to: PESQ, MOS, and PSQM
- Q13) B
Relates to: PESQ, MOS, and PSQM
- Q14) C
Relates to: PESQ, MOS, and PSQM
- Q15) B
Relates to: Objectives of QoS
- Q16) B
Relates to: Objectives of QoS
- Q17) C, F
Relates to: Using QoS to Improve Voice Quality
- Q18) A, C

Relates to: Using QoS to Improve Voice Quality

Q19) D

Relates to: Recognizing Common Design Faults

Q20) B

Relates to: Recognizing Common Design Faults

Q21) D

Relates to: Cisco AutoQoS Features

Q22) B, C, D

Relates to: Cisco AutoQoS Features

Lesson 2

Implementing CAC

Overview

To prevent oversubscription of Voice over IP (VoIP) networks, the number of voice calls allowed on the network must be limited. This lesson describes the configuration parameters for implementing Call Admission Control (CAC).

Relevance

CAC must be implemented in a VoIP network to limit the use of bandwidth. Network administrators should understand the need for CAC and how to configure it.

Objectives

Upon completing this lesson, you will be able to configure call control on the network. This ability includes being able to meet these objectives:

- Describe the effects of bandwidth oversubscription on overall voice quality
- State the function of CAC as it relates to overall call control services
- Describe the operation of RSVP
- Describe the four distinct groups of CAC mechanisms
- Describe how H.323 implements CAC
- Describe how SIP implements CAC
- Describe how MGCP implements CAC
- State the two types of call admission that Cisco CallManager allows

Learner Skills and Knowledge

To benefit fully from this lesson, you must have these prerequisite skills and knowledge:

- Basic knowledge of VoIP
- Basic knowledge of TCP/IP networks

Outline

The outline lists the topics included in this lesson.

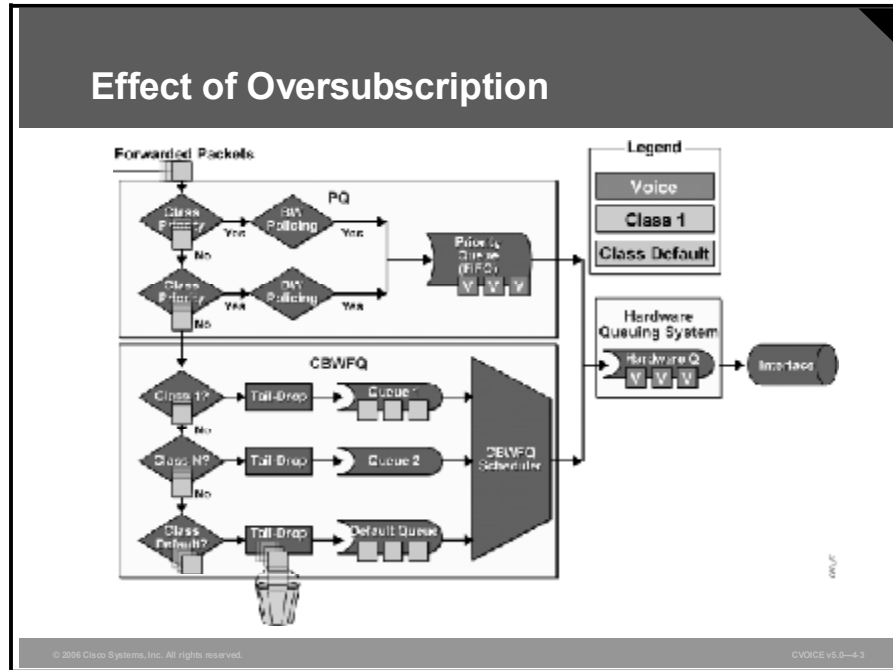
Outline

- **Overview**
- **Effects of Oversubscribing Bandwidth**
- **CAC Operation**
- **Resource Reservation Protocol**
- **CAC Tools**
- **H.323 CAC**
- **SIP CAC**
- **MGCP CAC**
- **Cisco CallManager CAC**
- **Summary**
- **Lesson Self-Check**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-62

Effects of Oversubscribing Bandwidth

This topic describes the effects of network link oversubscription.



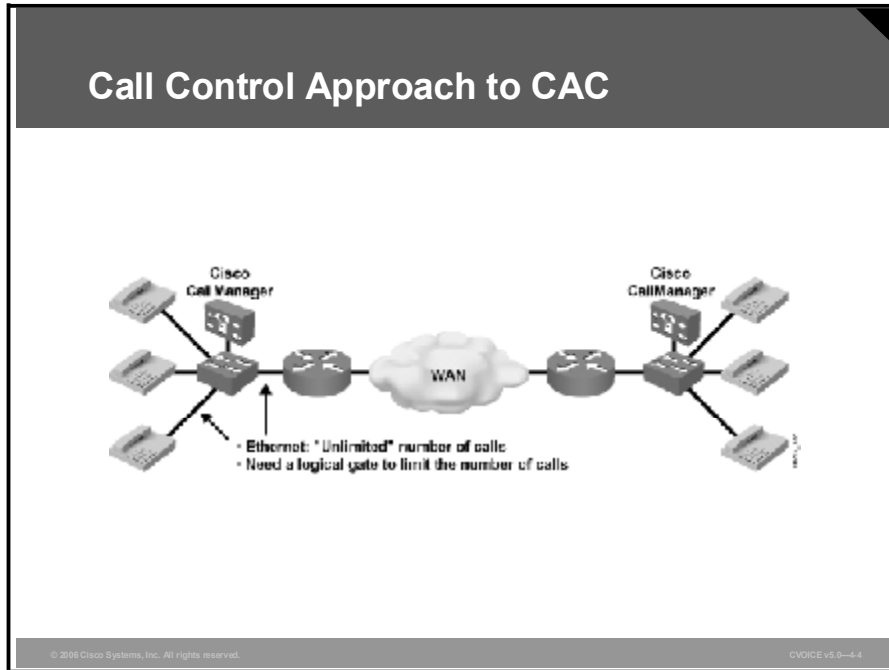
Quality of service (QoS) tools, such as queuing, ensure that voice traffic receives priority over data traffic. If a network link is oversubscribed with too much voice traffic, data packets are dropped, and the remaining voice calls suffer because they must compete for bandwidth from the low latency queue.

Example: Oversubscription

The figure illustrates the effect of voice oversubscription. Using Low Latency Queuing (LLQ), voice traffic is directed into one or more priority queues (PQs) while all other traffic is directed into various class-based weighted fair queuing (CBWFQ) queues. Note that PQs forward packets while the data packets, destined for the CBWFQ queues, are denied entry to the queue and are dropped. In the case shown in the diagram, even the PQ buffer is full and, therefore, the voice packets are competing with other voice packets for access to the network link. This situation will result in a degradation of all voice calls on this link.

CAC Operation

This topic describes the operation of CAC as a function of call control services.



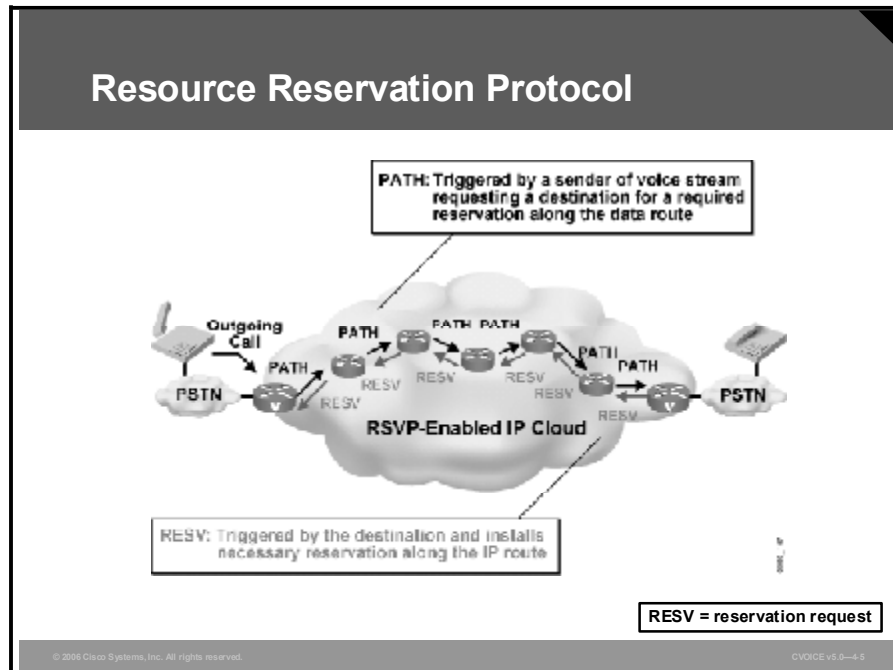
CAC, as part of call control services, functions on the outgoing gateway. CAC bases its decision on nodal information, such as the state of the outgoing LAN or WAN link. If the local packet network link is down, there is no point in executing complex decision logic based on the state of the rest of the network, because that network is unreachable. Local mechanisms include configuration items that disallow all calls that exceed a specified number.

Example: Call Control CAC

If the network designer already knows that bandwidth limitations allow no more than five calls across the outgoing WAN link, the local node can be configured to allow no more than five calls. You can configure this type of CAC on outgoing dial peers.

Resource Reservation Protocol

This topic describes the Resource Reservation Protocol (RSVP).



RSVP is the only CAC mechanism that makes actual bandwidth reservations for calls rather than making a call admission decision based on a best guess before the call is set up. This design 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. 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. At that point, the H.323 state machine continues with either 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 these important differences from other CAC methods discussed in this lesson:

- RSVP can maintain QoS for the duration of the call.
- RSVP is aware of topology. In concept, the RSVP reservation is installed on every interface that the call will traverse through the network. RSVP ensures bandwidth over every segment without any requirement of knowing the actual bandwidth provisioning on each interface or the path on which the routing protocols direct the packets. RSVP, therefore, adjusts automatically to network configuration changes, and no manual calculations are necessary to keep different aspects of the configuration synchronized.
- To function correctly, RSVP is dependent on the correct configuration for all devices in the network. (RSVP may introduce a scaling issue depending on how the network is designed.)
- RSVP provides an end-to-end reservation per call and has visibility for that call only. RSVP is unaware of how many other calls are active from a site or across an interface, or the source or destination of any other call.

Example: RSVP

Configuring RSVP in Cisco routers allows the administrator to limit the amount of bandwidth requested per call and the total amount of bandwidth allowed for all calls. This configuration is entered directly against the interface that will permit or deny the calls. The configuration also requires RSVP to be configured on the dial peers for the calls that will be managed by RSVP.

CAC Tools

This topic describes CAC tools available for various protocols and systems.

The slide has a dark grey header with the title 'Understanding CAC Tools' in white. Below the header is a white area with a bulleted list of four items. At the bottom of the slide, there is a small grey footer containing copyright information and a version number.

- **H.323 CAC**
- **SIP CAC**
- **MGCP CAC**
- **CallManager CAC**

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-4-8

As the many interesting aspects of CAC on packet networks have been considered, several different solutions have come into prominence—none of them solves the entire problem, but they all are useful to address a particular aspect of CAC. Unlike circuit-based networks, which reserve a free digital service level zero (DS0) time slot on every leg of the path that the call will take, determining whether a packet network has the resources to carry a voice call is not a simple undertaking.

Here are the four areas in which CAC may be implemented:

- H.323 CAC
- Session initiation protocol (SIP) CAC
- Media Gateway Control Protocol (MGCP) CAC
- Cisco CallManager CAC

Each area is associated with a specific protocol or system. Each of these areas will be explored in the next figures.

H.323 CAC

This topic describes the configuration options available for H.323 CAC.

H.323 CAC

- **call threshold** {*global trigger-name* | **interface** *interface-name interface-number int-calls*} **low** *value*
high *value* [**busyout** | **treatment**]
- **call spike** *call-number* [**steps** *number-of-steps* **size** *milliseconds*]
- **call treatment** {**on** | **action** *action* [*value*] | **cause-code** *cause-code* | **isdn-reject** *value*}

© 2006 Cisco Systems, Inc. All rights reserved.CVOICE v5.0-4-7

The CAC for the H.323 VoIP gateways feature allows you to configure thresholds for local resources, memory, and CPU resources.

With the **call threshold** command, you can configure two thresholds, high and low, for each resource. Call treatment is triggered when the current value of a resource exceeds 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 and provides hysteresis (a phenomenon in which the response of a physical system to an external influence depends not only on the present magnitude of that influence but also on the previous history of the system) in call admission decision making.

With the **call spike** command, you can configure the limit for incoming calls during a specified time period. A call spike occurs when a large number of incoming calls arrive from the public switched telephone network (PSTN) in a very short period of time; for example, 100 incoming calls in 10 ms.

With the **call treatment** command, you can 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:

- **Time-division multiplexing (TDM) hairpinning:** Hairpins the calls through the plain old telephone service (POTS) dial peer
- **Reject:** Disconnects the call
- **Play message or tone:** Plays a configured message or tone for the user

To enable the global resources of this gateway, use the **call threshold** command in global configuration mode. To disable this command, use the **no** form of this command.

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

no call threshold {global trigger-name | interface interface-
                 name int-calls}
```

Call Threshold Commands

Command	Description
<code>global trigger-name</code>	This command specifies the global resources on the gateway. The <i>trigger-name</i> arguments are as follows: <ul style="list-style-type: none"> ■ <i>cpu-5sec</i>: CPU utilization in the last 5 seconds ■ <i>cpu-avg</i>: Average CPU utilization ■ <i>io-mem</i>: I/O memory utilization ■ <i>proc-mem</i>: Processor memory utilization ■ <i>total-calls</i>: Total number of calls (The valid range is from 1 to 10,000.) ■ <i>total-mem</i>: Total memory utilization
<code>interface interface-name interface-number</code>	This command specifies the gateway. The types of interfaces and their numbers will depend upon the configured interfaces.
<code>int-calls</code>	This command specifies the number of calls through the interface. The valid range is from 1 call to 10,000 calls.
<code>low value</code>	This command specifies the value of low threshold. The valid range is from 1 percent to 100 percent for the utilization triggers.
<code>high value</code>	This command specifies the value of high threshold. The valid range is from 1 percent to 100 percent for the utilization triggers.
<code>busyout</code>	(Optional—global only) This command automatically buses out the T1/E1 channels if the resource is not available
<code>treatment</code>	(Optional—global only) This command applies call treatment from session application if the resource is not available

To configure the limit of incoming calls in a short period of time, use the **call spike** command in global configuration mode. To disable this command, use the **no** form of this command. The **call spike** command uses a sliding window to determine the period in which the spike is limited. The sliding window period is defined using the **size** command, with valid ranges from 100 ms to 250 ms. If a longer spike period is desired, the **steps** command is used as a multiplier for the **size** command. For example, if the **steps** were set to 2 and the **size** was set to 250, the spike period would be 500 ms.

```
call spike call-number [steps number-of-steps size
                       milliseconds]

no call spike
```

Call Spike Commands

Command	Description
<code>call-number</code>	Incoming call numbers for spiking threshold; valid range is from 1 to 2,147,483,647
<code>steps number-of-steps</code>	(Optional) Number of steps; valid range is from 3 to 10
<code>size milliseconds</code>	(Optional) Step size in milliseconds; valid range is from 100 to 2000

To configure how calls should be processed when local resources are unavailable, use the **call treatment** command in global configuration mode. To disable the call treatment triggers, use the **no** form of this command.

```
call treatment {on | action action [value] | cause-code cause-code | isdn-reject value}
no call treatment {on | action action [value] | cause-code cause-code | isdn-reject value}
```

Call Treatment Commands

Command	Description
<code>on</code>	Enables call treatment from default session application
<code>action action</code>	Action to take when call treatment is triggered The <i>action</i> argument has these possible values: <ul style="list-style-type: none">■ <i>hairpin</i>: Hairpin■ <i>playmsg</i>: Specifies the audio file to play (URL)■ <i>reject</i>: Disconnects the call and passes down the cause code
<code>value</code>	(Optional) (For the <i>action</i> <i>playmsg</i> argument only) Specifies the audio file to play; URL format
<code>cause-code cause-code</code>	Specifies the reason for disconnect to caller The <i>cause-code</i> argument can have these values: <ul style="list-style-type: none">■ <i>busy</i>: Indicates that the gateway is busy■ <i>no-QoS</i>: Indicates that the gateway cannot provide QoS■ <i>no-resource</i>: Indicates that the gateway has no resources available
<code>isdn-reject value</code>	Selects the ISDN rejection cause code The <i>value</i> argument has these values: <ul style="list-style-type: none">■ 34 through 47 (ISDN cause codes for rejection)

ISDN Cause Codes

Cause No.	Description	Function
34	No circuit available (circuit or channel congestion)	Indicates that there is no channel available to handle the call
38	Net out of order	Indicates that the network is not functioning properly and that the malfunction is likely to last a long time (Reattempting the call is not likely to be successful.)
41	Net problem, redial (temporary failure)	Indicates that the network is not functioning properly and that the malfunction is not going to last a long time (Reattempting the call is likely to be successful.)
42	Net busy, redial (switching equipment congestion)	Indicates that the switching equipment is experiencing high traffic load
43	Access or user information discarded	Indicates that the network is unable to deliver user information to the remote users as was requested
44	No channel available (requested circuit or channel not available)	Indicates that the circuit or channel indicated by the requesting side cannot be used by the other side of the interface
47	Resource unavailable or new destination	Indicates a resource unavailable event only when no other cause in the resource unavailable class applies

Example: H.323 CAC Configuration

This example will busy out the **total-calls** command if 5 (low) or 5000 (high) is reached:

```
call threshold global total-calls low 5 high 5000 busyout
```

This example enables thresholds of 5 (low) and 2500 (high) for interface calls on interface Ethernet 0:

```
call threshold interface Ethernet 0 int-calls low 5 high 2500
```

This example will busy out the average CPU utilization if 5 percent (low) or 65 percent (high) is reached:

```
call threshold global cpu-avg low 5 high 65 busyout
```

The configuration of the **call spike** command that follows has a call number of 30, 10 steps, and a step size of 2000 ms:

```
call spike 30 steps 10 size 2000
```

This example enables the call treatment feature with a hairpin action:

```
call treatment on  
call treatment action hairpin
```

This example displays proper formatting of the **playmsg action** keyword:

```
call treatment action playmsg tftp://keyer/prompts/congestion.  
au
```

Note The congestion.au file plays when local resources are not available to handle the call.

This example configures a call treatment cause code to display “no QoS” when local resources are unavailable to process a call:

```
call treatment cause-code no-qos
```


SIP CAC

This topic describes the configuration options available for session initiation protocol (SIP) CAC.

SIP CAC

- **SAA RTR Responder**
 - rtr responder
- **PSTN Fallback**
 - call fallback active
- **Resource availability check**
 - call threshold global *trigger-name* low *value* high *value* [busyout][treatment]
 - call treatment {on | action *action* [*value*] cause-code *cause-code* | isdn-reject *value*}
 - call threshold interface *interface-name* interface *number* int-calls low *value* high *value*

© 2006 Cisco Systems, Inc. All rights reserved. CVOICE v5.0-4-8

The measurement-based CAC for SIP features support within SIP to monitor IP network capacity and reject or redirect calls based on congestion detection. This feature performs these functions:

- Verifies that adequate resources are available to carry a successful VoIP session
- Implements a mechanism to prevent calls arriving from the IP network from entering the gateway when required resources are not available to process the call
- Supports measurement-based CAC processes

Configuring SAA RTR Responder

Service Assurance Agent (SAA) is a generic network management feature that provides a mechanism for network congestion analysis. SAA determines latency, delay, and jitter and provides real-time Calculated Planning Impairment Factor (CPIF) calculations before establishing a call across an IP infrastructure. The SAA Responder feature uses SAA probes to 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 to use in making a decision on the condition of the network and its ability to carry a call. Threshold values for rejecting a call are configured at the outgoing gateway.

Each probe consists of multiple packets, a configurable parameter of this feature. SAA packets emulate voice packets and receive the same priority as voice throughout the entire network. The delay, loss, and ICPIF values entered into the cache for the IP destination are averaged from all the responses. If the call uses G.729 and G.711 coder-decoders (codecs), the probe packet sizes mimic those of a voice packet for that codec. Other codecs use G.711-like probes. In Cisco IOS software releases later than Cisco IOS Release 12.1(3)T, other codec choices may also be supported with their own specific probes.

The IP precedence of the probe packets can also be configured to simulate 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.

SAA probes used for CAC go out randomly on ports selected from within the top end of the audio User Datagram Protocol (UDP)-defined port range (16384 to 32767). Probes use a packet size based on the codec that the call will use. IP precedence can be set if desired, and a full Real-Time Transport Protocol (RTP), UDP, or IP header is used, just as a real voice packet would carry. The SAA Responder feature was called Response Time Reporter (RTR) in earlier releases of Cisco IOS software.

Use the **rtr responder** command to enable SAA Responder functionality on the destination node.

Configuring PSTN Fallback

The measurement-based CAC for SIP feature supports PSTN Fallback, which monitors congestion in the IP network and either redirects calls to the PSTN or rejects calls based on network congestion. Calls can be rerouted to an alternate IP destination or to the PSTN if the IP network is found unsuitable for voice traffic at that time. You can define congestion thresholds based on the configured network. This functionality allows the service provider to give a reasonable guarantee about the quality of the conversation to VoIP users at the time of call admission.

Note PSTN Fallback does not provide assurances that a VoIP call that proceeds over the IP network is protected from the effects of congestion. This is the function of the other QoS mechanisms, such as IP RTP or LLQ.

PSTN Fallback includes these capabilities:

- PSTN Fallback provides the ability to define the congestion thresholds based on the network.
 - Defines a threshold based on ICPIF, which is derived as part of ITU G.113
 - Defines a threshold based solely on packet delay and loss measurements
- PSTN Fallback uses SAA probes to provide packet delay, jitter, and loss information for the relevant IP addresses. Based on the packet loss, delay, and jitter encountered by these probes, an ICPIF or delay or loss value is calculated.
- PSTN Fallback supports calls of any codec. Only G.729 and G.711 have accurately simulated probes. Calls of all other codecs are emulated by a G.711 probe.

The call fallback subsystem has a network traffic cache that maintains the ICPIF or delay or loss values for various destinations. This capability helps performance, because each new call to a well-known destination need not wait for a probe to be admitted because the value is usually cached from a previous call.

Once the ICPIF or delay or loss value is calculated, it is stored in a fallback cache where it remains until the cache ages out or overflows. Until an entry ages out, probes are sent periodically for that particular destination. This time interval is configurable.

To configure PSTN Fallback, use this command:

```
call fallback active
```

This command enables a call request to fall back to alternate dial peers in case of network congestion. The **active** keyword enables a call request to fall back to alternate dial peers in case of network congestion.

Configuring Resource Availability Check

User-selected thresholds allow you to configure call admission thresholds for local resources and end-to-end memory and CPU resources. You can configure two thresholds, high and low, for each global or interface-related resource. The specified call treatment is triggered when the current value of a resource goes beyond the configured high and remains in effect until the current resource value falls below the configured low.

You can 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 exceeds the configured threshold, you have these call treatment choices:

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

To configure resource availability checking, use this command:

```
call threshold global trigger-name low value high value  
[busyout] [treatment]
```

This command enables a trigger and defines associated parameters to allow or disallow new calls on the router. Action is enabled when the trigger value exceeds the value specified by the **high** keyword and is disabled when the trigger value drops below the value specified by the **low** keyword.

Call Threshold Global Commands

Command	Description
<i>trigger-name</i>	The <i>trigger-name</i> argument can be one of the following: <ul style="list-style-type: none">■ cpu-5sec: CPU utilization in the last 5 seconds■ cpu-avg: Average CPU utilization■ io-mem: I/O memory utilization■ proc-mem: Processor memory utilization■ total-calls: Total number of calls■ total-mem: Total memory utilization
low <i>value</i>	Value of low threshold; range is from 1 percent to 100 percent for utilization triggers and from 1 to 10,000 for total calls
high <i>value</i>	Value of high threshold; range is from 1 percent to 100 percent for utilization triggers and from 1 to 10,000 for total calls
busyout	(Optional) Busies out the T1 or E1 channels if the resource is not available
treatment	(Optional) Applies call treatment from the session application if the resource is not available

To configure call treatment, use this command:

```
call treatment {on | action action [value] | cause-code cause-code | isdn-reject value}
```

This command configures how calls should be processed when local resources are unavailable.

Call Treatment Commands

Command	Description
<code>on</code>	This command enables call treatment from the default session application
<code>action action</code>	<p>This command specifies the action to be taken when call treatment is triggered.</p> <p>The <i>action</i> argument can have one of these values:</p> <ul style="list-style-type: none">■ hairpin: Specifies hairpinning action■ playmsg: Specifies that the gateway play the selected message (The optional <i>value</i> argument specifies the audio file to play in URL format.)■ reject: Specifies whether the call should be disconnected and the ISDN cause code passed
<code>cause-code cause-code</code>	<p>This command specifies the reason for disconnection to the caller.</p> <p>The <i>cause-code</i> argument can have one of these values:</p> <ul style="list-style-type: none">■ busy: Indicates that the gateway is busy■ no-QoS: Indicates that the gateway cannot provide QoS■ no-resource: Indicates that the gateway has no resources available
<code>isdn-reject value</code>	This command applies to ISDN interfaces only and specifies the ISDN reject cause code. The range for the <i>value</i> argument is 34 to 47 (ISDN cause code for rejection).

To configure resource availability checking for interface resources, perform the following task:

```
call threshold interface interface-name interface number int-calls low value high value
```

This command allows threshold values to be configured for total numbers of voice calls placed through a particular interface. This command is used to allow or disallow admission for new calls on the router.

Call Threshold Interface Commands

Command	Description
<i>interface-name</i>	This argument specifies the interface used in making call admission decisions. The types of interfaces and their numbers will depend upon the configured interfaces.
<i>interface-number</i>	This argument specifies the number of calls through the interface that triggers a call admission decision.
int-calls	This command configures the gateway to use the number of calls through the interface as a threshold.
low	This command enables the specified call treatment until the number of calls through the interface drops below the configured <i>low value</i> argument. The <i>value</i> argument specifies the number of calls used to make call admission decisions. The range is from 1 to 10,000 calls.
high	This command enables the specified call treatment until the number of calls through the interface exceeds the configured <i>high value</i> argument. The <i>value</i> argument specifies the number of calls used to make call admission decisions. The range is from 1 to 10,000 calls.

Example: SIP CAC Configuration

Here are examples of uses of the SIP CAC commands:

- SAA RTR Responder:

```
Router(config)# rtr responder
```

- PSTN Fallback:

```
Router(config)# call fallback active
```

- Resource availability checking:

```
Router(config)# call threshold global total-calls low 5 high  
1000 busyout
```

```
Router(config)# call treatment action cause-code 17
```

```
Router(config)# call threshold interface ethernet 0 int-calls  
low 5 high 2500
```

MGCP CAC

This topic describes the configuration options available for MGCP CAC.

MGCP CAC

- System Resource Check (SRC) CAC**
 - **call threshold global** *trigger-name low value high value treatment*
- Resource Reservation Protocol (RSVP) CAC**
 - **ip rsvp bandwidth** [*interface-kbps [single-flow-kbps]*]
- Cisco Service Assurance Agent (SAA) CAC**
 - **call fallback active**
 - **mgcp rtrcac**
 - **rtr responder**

© 2006 Cisco Systems, Inc. All rights reserved.CVoice v5.0—4-5

The MGCP VoIP CAC feature enables certain Cisco CAC capabilities on VoIP networks that are managed by MGCP call agents. These capabilities permit the gateway to identify and gracefully refuse calls that are susceptible to poor voice quality.

Poor voice quality on an MGCP voice network can result from transmission artifacts such as echo, from the use of low-quality codecs, from network congestion and delay, or from overloaded gateways. The first two causes can be overcome by using echo cancellation and better codec selection. The last two causes are addressed by MGCP VoIP CAC.

Before the release of MGCP VoIP CAC, MGCP voice calls were often established regardless of the availability of resources for those calls in the gateway and the network. MGCP VoIP CAC ensures resource availability by disallowing calls when gateway and network resources are below configured thresholds and by reserving guaranteed bandwidth throughout the network for each completed call.

MGCP VoIP CAC has these three components for improving voice quality and reliability:

- System resource check (SRC) CAC evaluates memory and call resources local to the gateway. SRC CAC is supported in MGCP 1.0 and MGCP 0.1.
- RSVP CAC surveys bandwidth availability on the network. RSVP CAC is supported in MGCP 1.0 and MGCP 0.1.
- Cisco SAA CAC appraises network congestion conditions on the network. Cisco SAA CAC is supported only in MGCP 1.0.

Configuring SRC CAC

To set thresholds and enable MGCP SRC CAC, use this command in global configuration mode:

```
call threshold global trigger-name low value high value
                        treatment
```

This command enables a resource and defines its parameters. Treatment of attempted calls is enabled when the resource cost goes beyond the high value. Treatment is not disabled until the resource cost drops below the low value. The arguments and keywords are shown in the table.

Call Threshold Global Commands

Command	Description
<i>trigger-name</i>	The <i>trigger-name</i> argument can have one of these values: <ul style="list-style-type: none">■ cpu-5sec: CPU utilization in the last 5 seconds■ cpu-avg: Average CPU utilization■ io-mem: I/O memory utilization■ proc-mem: Processor memory utilization■ total-calls: Total number of calls■ total-mem: Total memory utilization
low <i>value</i>	Value of low threshold; range is from 1 percent to 100 percent for utilization triggers and from 1 to 10,000 for total calls
high <i>value</i>	Value of high threshold; range is from 1 percent to 100 percent for utilization triggers and from 1 to 10,000 for total calls
treatment	(Optional) Applies call treatment from the session application if the resource is not available

If network conditions rise above the high threshold value, SRC rejects the call by sending the call agent an MGCP error message with the return code 403. The call agent applies a treatment to the rejected call.

Configuring RSVP CAC

To configure MGCP RSVP CAC on a media gateway, use this command in global configuration mode:

```
ip rsvp bandwidth (interface-kbps [single-flow-kbps])
```

This command enables RSVP for IP on an interface. RSVP is disabled by default. It should be noted that for RSVP to operate correctly end to end, it must be configured on all routers in the network. The arguments are shown in the table.

IP RSVP Bandwidth Commands

Command	Description
<i>interface-kbps</i>	(Optional) This sets the maximum amount of bandwidth, in kilobits per second, that may be allocated by RSVP flows. The range is from 1 to 10,000,000. This parameter should be configured for the maximum amount of voice bandwidth that this interface is limited to for all total calls.
<i>single-flow-kbps</i>	(Optional) This sets the maximum amount of bandwidth, in kilobits per second, that may be allocated to a single flow. The range is from 1 to 10,000,000. This parameter should be configured for the amount of bandwidth for one call.

Configuring Cisco SAA CAC

Cisco SAA is an application-aware synthetic operation agent that monitors network performance by measuring response time, network resource availability, application performance, jitter (interpacket delay variance), connect time, throughput, and packet loss. Performance can be measured between any Cisco device that supports this feature and any remote IP host (server), Cisco routing device, or mainframe host. Performance measurement statistics provided by this feature can be used for troubleshooting, problem analysis, and designing network topologies.

The SAA Responder that is enabled using the **rtr responder** command is a component embedded in the target Cisco routing device that allows the system to anticipate and respond to SAA request packets. The SAA Responder can listen on any user-defined port for UDP and TCP protocol messages. In client-server terminology, the SAA Responder is a concurrent multiservice server.

The commands to configure Cisco SAA CAC are as follows:

- **call fallback active:** Enables a call request to fall back to alternate dial peers in case of network congestion
- **mgcp rtrcac:** Enables MGCP SAA CAC
- **rtr responder:** Enables the SAA responder functionality on a Cisco device

Example: MGCP VoIP CAC on a Trunking Gateway

This configuration enables all three types of MGCP VoIP CAC: SRC, RSVP, and SAA. Comment lines are provided above the CAC commands to help you identify the commands needed for a particular CAC type.

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname eastcoast
!
!
voice-card 2
!
voice-card 3
!
ip subnet-zero
ip dhcp smart-relay
!
! The following command is used in MGCP SA Agent CAC.
call fallback active
! The following command is used in MGCP RSVP CAC.
call rsvp-sync
! The following six commands are used in MGCP SRC CAC.
call threshold global cpu-5sec low 55 high 70 treatment
call threshold global cpu-avg low 70 high 80 treatment
call threshold global total-mem low 70 high 80 treatment
call threshold global io-mem low 70 high 80 treatment
call threshold global proc-mem low 70 high 80 treatment
call threshold global total-calls low 10 high 12 treatment
!
controller T1 2/0
!
controller T1 2/1
!
controller T1 3/0
framing esf
clock source internal
ds0-group 1 timeslots 1-5 type none service mgcp
ds0-group 2 timeslots 6-24 type none service mgcp
```

```

!
controller T1 3/1
    framing esf
    ds0-group 1 timeslots 1-10 type none service mgcp
    ds0-group 2 timeslots 11-24 type none service mgcp
!
!
!
interface FastEthernet0/0
    ip address 192.168.1.61 255.255.255.0
    duplex auto
    speed auto
! The following command is used in MGCP RSVP CAC to configure
the bandwidth allocated.
! for VoIP calls through the interface.
    ip rsvp bandwidth 512 512
!
interface FastEthernet0/1
    ip address 172.20.1.1 255.255.0.0
    duplex auto
    speed auto
!
ip kerberos source-interface any
ip classless
ip route 10.0.0.0 10.0.0.0 192.168.1.10
no ip http server
!
snmp-server engineID local 0000000902000002B95D89F0
no snmp-server ifindex persist
snmp-server manager
!
voice-port 3/0:1
!
voice-port 3/0:2
!
voice-port 3/1:1
!
voice-port 3/1:2
!
mgcp
mgcp call-agent 10.13.57.88 service-type mgcp version 1.0

```

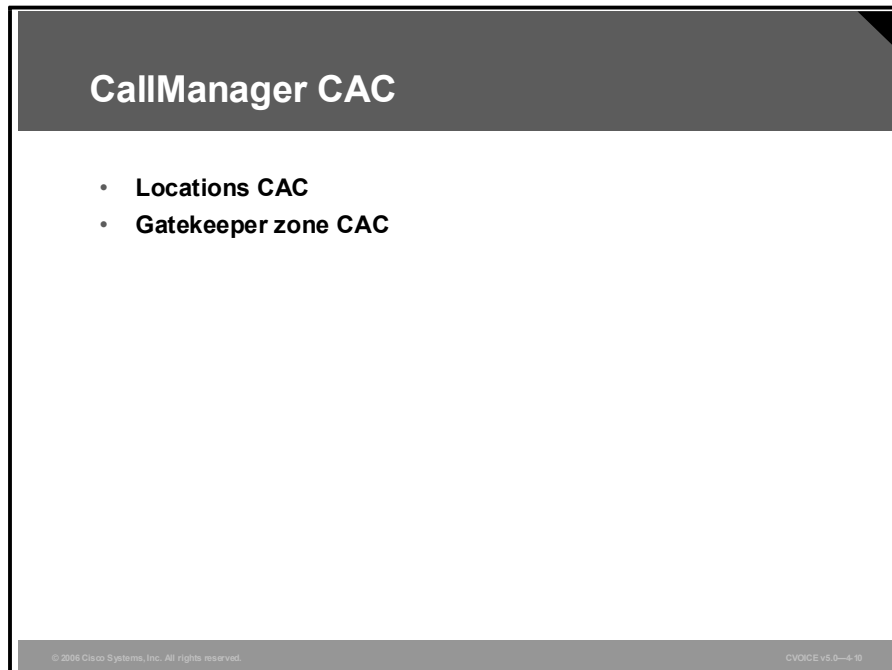
```

mgcp modem passthrough voip mode nse
mgcp modem passthrough voaal2 mode
mgcp package-capability trunk-package
! The following command is used for MGCP SA Agent CAC.
mgcp rtrcac
! The following command is used in MGCP SRC CAC.
mgcp src-cac
no mgcp timer receive-rtcp
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 1 pots
  application mgcpapp
  port 3/0:1
!
dial-peer voice 2 pots
  application mgcpapp
  port 3/0:2
!
dial-peer voice 3 pots
  application mgcpapp
  port 3/1:1
!
dial-peer voice 4 pots
  application mgcpapp
  port 3/1:2
!
! The following command is used in MGCP SA Agent CAC.
rtr responder.
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line vty 0 4
  login
!
end

```

Cisco CallManager CAC

This topic describes the types of call admission that are possible with Cisco CallManager CAC.



Using Cisco CallManager, these two types of call admission are possible:

- **Locations CAC:** The locations feature provides CAC for centralized call-processing systems. A centralized system uses a single Cisco CallManager cluster to control all of the locations. The locations feature in Cisco CallManager allows you to specify the maximum amount of bandwidth available for calls *to* and *from* each location, thereby limiting the number of active calls and preventing oversubscription of the bandwidth on the IP WAN links.
- **Gatekeeper zone CAC:** A gatekeeper device provides CAC for distributed call-processing systems. In a distributed system, each site contains its own call-processing capability. Calls are limited between zones in this configuration.

Summary

This topic summarizes the key points discussed in this lesson.

Summary

- **If a network link is oversubscribed with too much voice traffic, data packets are dropped and voice calls suffer.**
- **CAC functions as part of call control services.**
- **RSVP is a CAC mechanism.**
- **Various CAC tools are available for different protocols and systems.**
 - **Cisco provides for H.323 Call Admission Control.**
 - **Cisco provides for SIP Call Admission Control.**
 - **Cisco provides for MGCP Call Admission Control.**
 - **Cisco CallManager allows for two types of call admission.**

References

For additional information, refer to these resources:

- *VoIP Call Admission Control* (see section on Resource-Based CAC Mechanisms).
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/cac.htm#77341>.
- *Call Admission Control for H.323 VoIP Gateways*.
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800e0d4b.html#76206.
- *Measurement-Based Call Admission Control for SIP*.
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541b2.html.
- *MGCP VoIP Call Admission Control*.
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d37.html#1048015.

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) In which two ways is traffic affected if a link is oversubscribed for voice?
(Choose two.)
- A) Data packets continue to be sent but at a slower rate.
 - B) Data packets are denied entry to the queue.
 - C) Voice packets compete for bandwidth with other packets from the priority queue.
 - D) Voice packets are sent as priority traffic and dropped packets are retransmitted.
- Q2) If CAC and LLQ are enabled on a link, which traffic will be transmitted first?
- A) small data packets
 - B) large data packets
 - C) voice packets
 - D) packets that arrived first
- Q3) At what location in the network are CAC call control services configured?
- A) the incoming gateway
 - B) the outgoing gateway
 - C) the incoming gatekeeper
 - D) the outgoing gatekeeper
 - E) the entire network
- Q4) Which statement describes CAC call control?
- A) The local node is configured to allow no more than a specified number of calls.
 - B) The local node routes the calls on links that have enough bandwidth.
 - C) The network does not allow calls that are not negotiated.
 - D) The network holds the link open until all priority calls have gone through.
- Q5) Which characteristic of RSVP is different from other CAC mechanisms?
- A) requires manual configuration at each interface in the path
 - B) denies a call based on a best guess
 - C) guarantees QoS against changing network conditions
 - D) knows how many other calls are active on the link
- Q6) Which device makes the CAC decision when RSVP is being used?
- A) the originating dial peer
 - B) the terminating dial peer
 - C) the originating gateway
 - D) the terminating gateway
- Q7) In a network that is supporting voice, in which two areas can CAC be implemented?
(Choose two.)
- A) H.323
 - B) SGCP
 - C) gatekeeper
 - D) SIP
 - E) H.245
 - F) H.225

- Q8) Each area of CAC is associated with a specific _____ or system.
- A) server
 - B) gateway
 - C) endpoint
 - D) protocol
- Q9) With the _____ command, you can configure two thresholds, high and low, for each resource.
- A) **call spike**
 - B) **call threshold**
 - C) **call treatment**
 - D) **rtr responder**
- Q10) With the _____ command, you can select how the call should be treated when local resources are not available to handle the call.
- A) **call spike**
 - B) **call threshold**
 - C) **call treatment**
 - D) **rtr responder**
- Q11) Which three factors does SAA use to monitor network performance?
(Choose three.)
- A) latency
 - B) codec availability
 - C) delay
 - D) jitter
 - E) bandwidth
- Q12) Which CAC tool monitors congestion in the IP network and either redirects calls to the PSTN or rejects calls based on network congestion?
- A) PSTN Fallback
 - B) SAA
 - C) resource availability checking
 - D) RSVP
- Q13) Which three components does MGCP VoIP CAC use for improving voice quality and reliability? (Choose three.)
- A) SRC
 - B) RSVP
 - C) DSCP
 - D) SAA
 - E) IP precedence
- Q14) To set thresholds and enable MGCP SRC CAC, which command is used in global configuration mode?
- A) **configure terminal**
 - B) **call-rsvp sync**
 - C) **call threshold global trigger-name low value high value treatment**
 - D) **call global threshold low value high value trigger-name treatment**

- Q15) Which two commands are necessary for SAA to monitor network performance with MGCP? (Choose two.)
- A) **rtr responder**
 - B) **mgcp rtrcac**
 - C) **call fallback active**
 - D) **mgcp src-cac**
 - E) **interface-kbps**
 - F) **single-flow-kbps**
- Q16) Which feature of Cisco CallManager allows you to specify the maximum bandwidth available for calls to and from each location?
- A) the set bandwidth feature
 - B) the locations feature
 - C) the gatekeeper zone feature
 - D) the active calls feature
- Q17) Which device provides CAC for distributed call processing using Cisco CallManager?
- A) DSP
 - B) dial peer
 - C) gatekeeper
 - D) gateway

Lesson Self-Check Answer Key

- Q1) B, C
Relates to: Effects of Oversubscribing Bandwidth
- Q2) C
Relates to: Effects of Oversubscribing Bandwidth
- Q3) B
Relates to: CAC Operation
- Q4) A
Relates to: CAC Operation
- Q5) C
Relates to: Resource Reservation Protocol
- Q6) D
Relates to: Resource Reservation Protocol
- Q7) A, D
Relates to: CAC Tools
- Q8) D
Relates to: CAC Tools
- Q9) B
Relates to: H.323 CAC
- Q10) C
Relates to: H.323 CAC
- Q11) A, C, D
Relates to: SIP CAC
- Q12) A
Relates to: SIP CAC
- Q13) A, B, D
Relates to: MGCP CAC
- Q14) C
Relates to: MGCP CAC
- Q15) A, B
Relates to: MGCP CAC
- Q16) B
Relates to: Cisco CallManager CAC
- Q17) C
Relates to: Cisco CallManager CAC

CVOICE

Cisco Voice over IP

Version 5.0

Lab Guide

QACS Production Services: 02.20.06

Copyright © 2006, 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 © 2006 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 2-1: Connecting a Voice-Enabled Router
- Lab 2-2: Configuring Voice Interfaces
- Lab 2-3: Configuring POTS Dial Peers
- Lab 2-4: Configuring Special-Purpose Connections
- Lab 2-5: Configuring Basic VoIP Network Connections
- Lab 3-1: Configuring VoIP with H.323
- Lab 3-2: Configuring VoIP with SIP
- Lab 3-3: Configuring VoIP with MGCP
- Lab 4-1: Implementing Cisco AutoQoS
- Lab 4-2: Implementing CAC
- Answer Key
- Lab Pull-Out Resource

Lab 2-1: Connecting a Voice-Enabled Router

Complete this lab activity to practice what you learned in the related module.

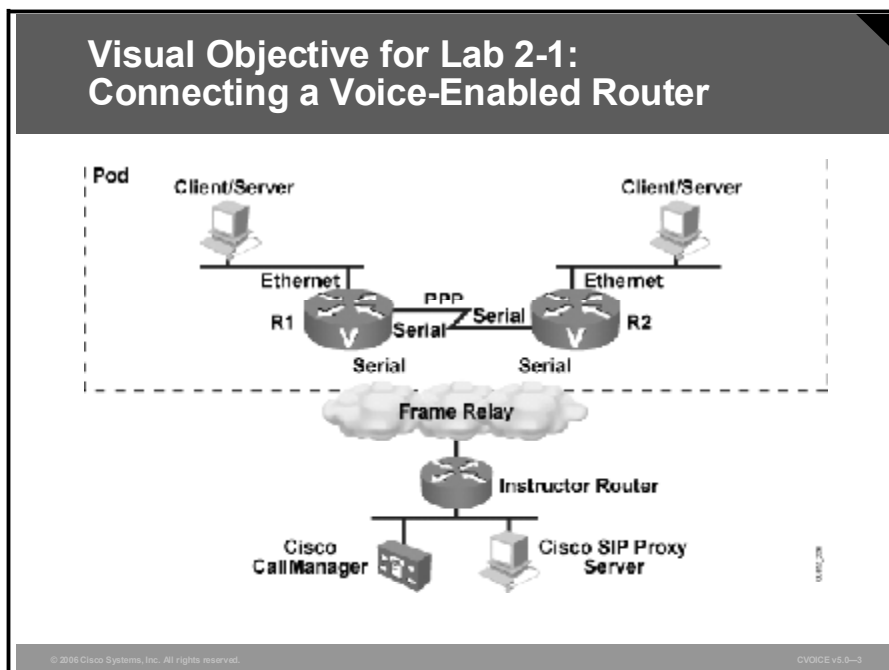
Activity Objective

In this activity, you will become familiar with the routers in your pod and the relationship of your pod with the other pods. You will also personalize your pod routers with host names and IP host tables and perform basic IP configuration to allow communication in and around the classroom. You will not be connecting any telephony hardware in this lab. After completing this activity, you will be able to meet these objectives:

- List the data interfaces and voice ports on your routers
- Refer to the other routers in your pod, and elsewhere, by aliases
- Access the client/servers in all other pods in the classroom
- Access the classroom servers

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

Each pod contains two complete sets of hardware and a shared PSTN simulator. These are the resources and equipment that are required to complete this activity:

- Two voice-enabled routers
- Two client/servers (laptop or desktop computers)
- Two Ethernet crossover cables
- Three serial crossover (DTE-DCE) cables

Command List

The table describes the commands that are used in this activity.

Activity Commands

Command	Description
<code>clock rate rate</code>	Configures the clock rate for the hardware connections on serial interfaces. This command is executed in interface configuration mode.
<code>configure terminal</code>	Enters configuration mode. This command is executed in privileged mode.
<code>copy running-config startup-config</code>	Copies current running configuration into NVRAM. This command is executed in privileged mode.
<code>enable</code>	Enters privileged mode. This command is executed in user mode.
<code>enable secret password</code>	Sets password to control access to privilege level. This command is executed in global configuration mode.
<code>encapsulation encaps-type</code>	Sets the encapsulation type. This command is executed in interface configuration mode.
<code>hostname name</code>	Assigns a name to the router. This command is executed in global configuration mode.
<code>interface [Ethernet, serial] n</code>	Enters interface configuration mode for the specified interface. This command is executed in global configuration mode.
<code>ip address ip-address mask</code>	Configures the IP address and mask. This command is executed in interface configuration mode.
<code>ip host hostname ip-address</code>	Creates an IP host table entry assigning a name to an IP address. This command is executed in global configuration mode.
<code>line vty 0 4</code>	Enters vty line configuration mode for lines 0 through 4. This command is executed in global configuration mode.

Command	Description
logging synchronous	Redisplays the current line after a logging message has been displayed onscreen. Use this command for console or vty lines for cleaner display.
login	Enables password checking at login. This command is executed in line configuration mode.
network <i>network-address</i>	Specifies a list of networks for the EIGRP routing process. This command is executed in router configuration mode.
no auto-summary	Disables autosummarization and sends subprefix routing information across classful network boundaries. This command is executed in router configuration mode.
no ip domain-lookup	Disables DNS lookups. This command is executed in global configuration mode.
password <i>password</i>	Sets a password. This command is executed in line configuration mode.
ping (<i>ip-address or host name</i>)	Tests the reachability of a device. When in user mode, this command sends five default ping packets to test reachability. When in privileged mode, type in only the command ping <enter> to enter extended ping mode. The user can customize ping parameters for testing.
router eigrp <i>as-number</i>	Configures the EIGRP routing process. This command is executed in global configuration mode.
show controller t1	Displays controller status and statistics. This command is executed in user mode.
show ip interface brief	Displays a summary of interface status and IP addresses. This command is executed in user mode.
show ip route	Displays the IP routing table. This command is executed in user mode.
show version	Displays the hardware configuration, software version, names, and sources of configuration files and boot images. This command is executed in user mode.
show voice port summary	Displays a summary of all voice ports. This command is executed in user mode.
traceroute	Discovers the routes that packets take to a remote destination and where routing breaks down. When in user mode, this command sends three packets for each hop. When in privileged mode, type in only the command traceroute <enter> to enter extended trace route mode. The user can customize trace route parameters for testing.

Job Aids

These job aids are available to help you complete the lab activity.

IP Addressing Conventions

An IP addressing strategy has been adopted that allows the student to predict the address of any other device without knowing it beforehand. The table contains evidence of these conventions:

- Where x = pod number, y = host, addresses follow the format $10.x.10.y / 24$ for R1 Ethernet; $10.x.20.y / 24$ for R2 Ethernet; and $10.x.x.y / 24$ for PPP link.
- The Frame Relay network is modeled as a fully meshed, NBMA network using network 192.168.1.0.

In addition, the instructor Ethernet uses addresses in network 192.168.100.0.

IP Address Assignment

Pod Number	Device	Client	Ethernet	PPP	Frame Relay
1	R1	10.1.10.100	10.1.10. 1	10.1.1.1	192.168.1.11
	R2	10.1.20.100	10.1.20.1	10.1.1.2	192.168.1.12
2	R1	10.2.10.100	10.2.10.1	10.2.2.1	192.168.1.21
	R2	10.2.20.100	10.2.20.1	10.2.2.2	192.168.1.22
3	R1	10.3.10.100	10.3.10.1	10.3.3.1	192.168.1.31
	R2	10.3.20.100	10.3.20.1	10.3.3.2	192.168.1.32
4	R1	10.4.10.100	10.4.10.1	10.4.4.1	192.168.1.41
	R2	10.4.20.100	10.4.20.1	10.4.4.2	192.168.1.42

Host Name

Pod Number	Router	Host Name
1	R1	Pod1R1
	R2	Pod1R2
2	R1	Pod2R1
	R2	Pod2R2
3	R1	Pod3R1
	R2	Pod3R2
4	R1	Pod4R1
	R2	Pod4R2
5	R1	Pod5R1
	R2	Pod5R2
6	R1	Pod6R1
	R2	Pod6R2

Task 1: Initial Configuration

In this task, you will discover and configure the interfaces connecting to other equipment.

Activity Procedure

Complete these steps:

Step 1 Using the client/server, connect to the console port of your router.

Note Do *not* use the Setup dialog box to configure the router. When prompted, answer appropriately to exit setup mode and get to the router prompt.

Step 2 Identify the Cisco IOS software version and its features.

List the number of available interfaces.

Ethernet _____

Serial _____

Channelized T1/PRI _____

Voice _____ Type _____

Step 3 Use the appropriate commands to determine which Ethernet and serial interfaces are available and their interface numbers. Note the interface numbers here.

Ethernet _____, _____

Serial _____, _____

T1 _____, _____

Step 4 Use the appropriate commands to determine which voice ports are available and their port numbers. Note the type and port numbers here.

Type _____ Port number _____

Type _____ Port number _____

Type _____ Port number _____

Type _____ Port number _____

Step 5 To prepare for configuration, fill in the diagram here. The instructor will tell you which interfaces to use when connecting to the Frame Relay switch or router. For the Frame Relay link, connect the DTE end of the cable to your interface and the DCE end to the Frame Relay switch or router. For the PPP connection between the voice-enabled routers in the pod, configure R1 to be the DTE side and R2 to be the DCE side of the connection.

R1	Interface Number	IP Address	DTE/DCE
PPP Serial			
Frame Serial			
Ethernet			—
Frame Switch		—	

- Step 6** Configure your router host name with the appropriate name from the Host Name table in the Job Aids section. Configure an IP host table for other routers in the classroom. Configure the privileged password to be “san-fran”. Configure vty lines to allow password checking at login and the Telnet password to be “router”.
- Step 7** Connect serial interfaces as per the lab diagram using DTE-DCE cables. Remember, clock rate must be configured on the DCE side. Set the link speed to be 72,000 bps.
- Step 8** Configure both serial interfaces with correct encapsulations and IP addresses. See the IP Address Assignment table in the Job Aids section for address and encapsulation assignment. Configure one Ethernet interface with the correct IP address.
- Step 9** Connect the client/server Ethernet to the router Ethernet port using a crossover cable. Configure the IP address on the client/server, pointing the gateway to the router Ethernet address. Test connectivity by pinging your router. If you are unable to ping the router from the client/server, check to ensure that the speed and duplex settings match on both sides of the connection.
- Step 10** Enable EIGRP routing for autonomous system (AS) 100 and disable autosummarization. Enable EIGRP for all three of your interfaces.
- Step 11** View the routing table and compare it to the lab diagram.
- Step 12** Test IP reachability throughout the classroom by pinging or tracing from your client/server to other client/servers.
- Step 13** Save your configuration.

Activity Verification

You have completed this task when you attain these results:

- You see all other classroom subnetworks in your IP routing table.
- You can trace or ping from your client/server to all other client/servers in the classroom.

Lab 2-2: Configuring Voice Interfaces

Complete this lab activity to practice what you learned in the related module.

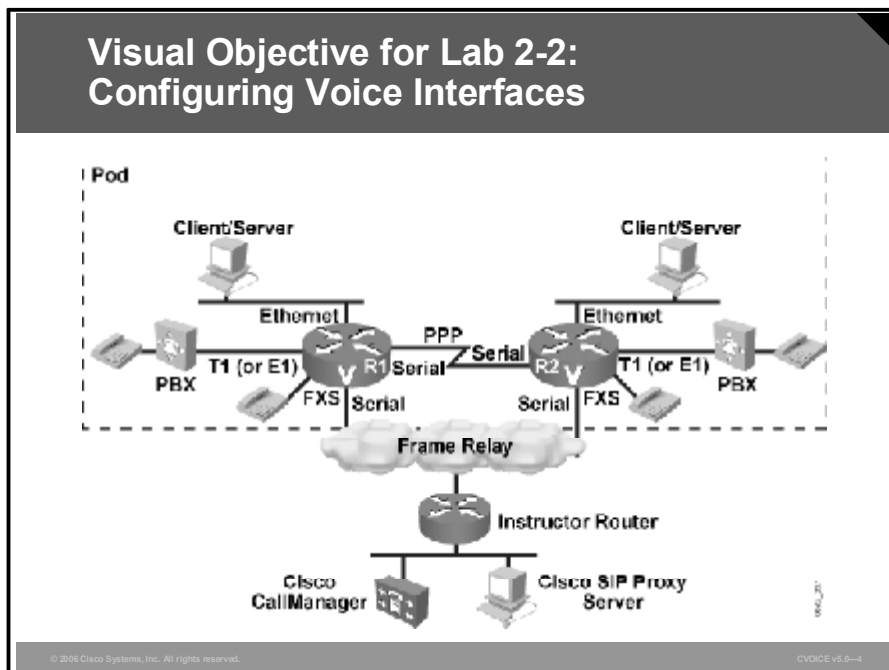
Activity Objective

In this activity, you will become familiar with existing analog voice ports. You will learn how to customize your analog ports by configuring various port parameters. You will also create and customize digital voice ports that connect to your PBX. After completing this activity, you will be able to meet these objectives:

- Identify default voice port settings
- Customize and verify analog port operations
- Create, customize, and verify digital port operations

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:

- Two T1 crossover cables
- Two PBX devices
- Four telephones
- Four RJ-11 cables

Command List

The table describes the commands that are used in this activity.

Voice Port Commands

Command	Description
<code>clock source source</code>	Specifies the clock source. This command is executed in controller configuration mode.
<code>controller t1 n</code>	Enters T1 controller configuration mode for the specified controller. This command is executed in global configuration mode.
<code>cptone country-code</code>	Sets the regional analog voice interface-related tone, ring, and cadence setting. This command is executed in voice-port configuration mode.
<code>default parameter</code>	Resets the value of the parameter to its default value. This command is executed in various configuration modes.
<code>ds0-group tag timeslots timeslot-list type signaling-type</code>	Specifies the DS0 timeslots that make up a logical voice port on a T1 or E1 controller and the signaling type for the DS0 group. This command is executed in controller configuration mode.
<code>framing sf/esf</code>	Specifies the framing type. This command is executed in controller configuration mode.
<code>linecode ami/b8zs</code>	Specifies the line code setting. This command is executed in controller configuration mode.
<code>ring cadence define pulse interval</code>	Sets the ring cadence for the FXS port. This defines how the telephone will ring. This command is executed in voice-port configuration mode.
<code>show voice port (summary)</code>	Views the voice port status and settings. Displays all default settings for each port. Specify a particular voice port to view only its settings. Use the summary option to view a summary table of the voice ports. This command is executed in user mode.
<code>timeouts initial secs</code>	Sets the number of seconds that the system will wait for the caller to input the first digit. This command is executed in voice-port configuration mode.
<code>voice-port port-number</code>	Enters voice-port configuration mode. This command is executed in global configuration mode.

Job Aids

These job aids are available to help you complete the lab activity.

PBX Configuration

The PBX parameters are as follows:

- T1 connection
- Timeslots 1–24
- E&M Wink-Start signaling
- Clock source is line
- ESF framing
- B8ZS line code

Task 1: Analog Voice Port Configuration

In this task, you will examine analog voice ports and configure voice port parameters.

Activity Procedure

Complete these steps:

- Step 1** Connect both phones to your voice-enabled router using RJ-11 cables.
- Step 2** Verify that the connections are correct by lifting the handset on both telephones and listening for the dial tone. If the dial tone is not present, troubleshoot the problem. Make sure that the router is powered on and that the cable is firmly seated. If the problem persists, ask your instructor for help.
- Step 3** Using **show** commands, identify the available voice ports, their type, and their default settings. Please note that not all settings are applicable to all types of ports; for example, ring frequency and ring cadence only apply to FXS ports. Record the information here.

	Voice Port 1	Voice Port 2	Voice Port 3	Voice Port 4
Port type	_____	_____	_____	_____
Port number	_____	_____	_____	_____
Operational state	_____	_____	_____	_____
Echo cancellation	_____	_____	_____	_____
Echo cancel coverage	_____	_____	_____	_____
Initial timeout	_____	_____	_____	_____
Region tone	_____	_____	_____	_____
Signal type	_____	_____	_____	_____

Ring frequency _____

Ring cadence _____

Step 4 Because many companies have international offices, it is important to know how to configure the voice port to match the standard signaling of a country. For this step, assume that you are configuring this router for Australia. On the FXS port that your telephone is connected to, configure the call progress tone setting for Australia. Notice that when you change the call progress tone setting, it automatically changes the ring cadence setting to match. Test the change by lifting the handset. You should hear a different dial tone.

Verify the changes with **show** commands and record the new settings here.

Region tone _____

Ring cadence _____

Once you have tested the tones for Australia, experiment with settings for other countries.

Step 5 What is the default initial timeout setting from Step 3? _____
On the FXS port that your telephone is connected to, change the initial timeout value to 4 seconds. Lift the handset and listen for more than 4 seconds. Can you dial digits after the dial tone stops? _____ Reset the initial timeout to the default.

Step 6 Because you will be working with two telephones all week, you may want one telephone to have a distinctive ring. Configure the ring cadence on your FXS port using the **define** option. You will be able to test this ring cadence in the next lab. What ring cadence did you define? _____

Activity Verification

You have completed this task when you attain this result:

- You have configured and verified analog voice port parameters.

Task 2: Digital Voice Port Configuration

In this task, you will configure your T1 to connect to your PBX device. In the process of configuring the T1 for voice calls, a logical voice port will be created. You will be able to view this newly created digital voice port with the same commands as for analog ports.

Activity Procedure

Complete these steps:

Step 1 Connect the PBX device to your router T1 interface with a crossover T1 cable. What port is your T1 cable plugged into? _____

Step 2 Use the **show controller T1** command to view the default settings for framing, line code, and clock source. Note these settings here.

Framing _____

Line code _____

Clock source _____

Step 3 Configure your T1 controller to complement the settings of the PBX as shown in the Job Aids section. Remember that because this is a back-to-back T1 connection, one side should have clock source line, and the other side should have clock source internal.

Verify that the settings match by checking that both controller LEDs are green. Use the **show controller T1** command to view status and new settings.

Step 4 When the T1 is functional, create digital voice ports using the **DS0-group** command. Once again, these settings must complement those of the connected PBX. Check the required settings in the Job Aids section of this lab. Configure the DS0 group and use **show** commands to verify the newly created digital voice port. Fill in the information here.

How many voice ports were created? _____

What is the voice port number? _____

How many channels were created? _____

Which command would you use to view the voice port and the channels?

What is the current status of these channels? _____

Step 5 Save your configuration.

Activity Verification

You have completed this task when you attain these results:

- You have verified the T1 connection to the PBX.
- You have verified the existence of the newly created digital voice port.

Lab 2-3: Configuring POTS Dial Peers

Complete this lab activity to practice what you learned in the related module.

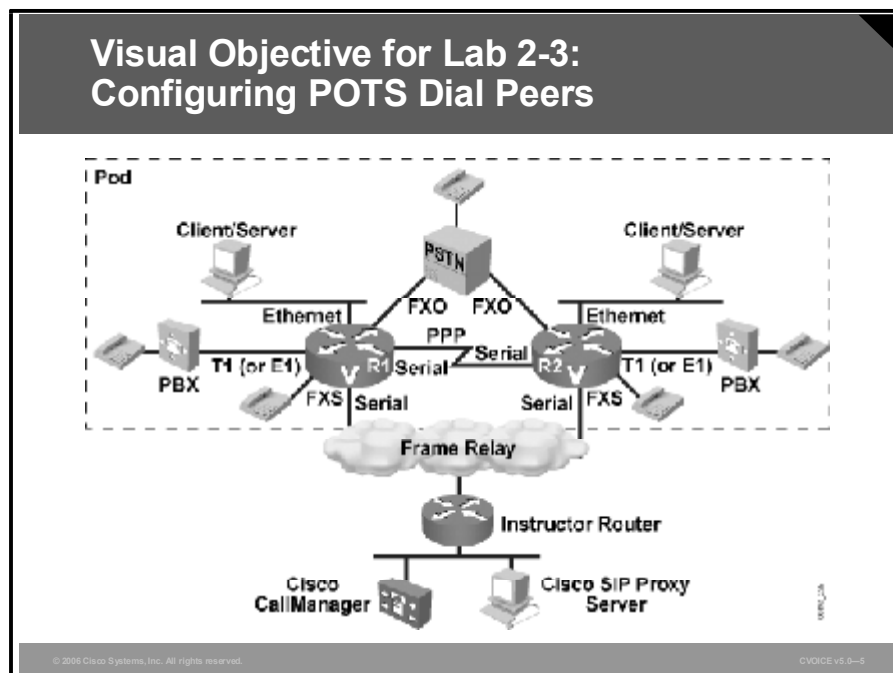
Activity Objective

In this activity, you will configure POTS dial peers to establish locally terminated calls, calls through a PBX, and calls to the PSTN. You will also experiment with two different configurations to control hunt capabilities. After completing this activity, you will be able to meet these objectives:

- Configure dial peers for locally terminated calls, PBX calls, and PSTN calls
- Determine the appropriate method of digit forwarding and manipulation
- Create hunt groups and determine hunting behavior

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment that each pod requires to complete this activity:

- One PSTN device
- One telephone
- Three sets of RJ-11 cables

Command List

The table describes the commands that are used in this activity.

Dial Peer Commands

Command	Description
<code>debug vpm signal</code>	Displays real-time voice port module signaling; displays digits as they are received by the voice port. This command is executed in privileged mode.
<code>destination-pattern string</code>	Configures a telephone number for this dial peer. This command is executed in dial-peer configuration mode.
<code>dial-peer hunt 0-7</code>	Specifies a hunt selection order for dial peers. This command is executed in global configuration mode.
<code>dial-peer voice tag pots</code>	Enters dial-peer configuration mode. This command is executed in global configuration mode.
<code>forward-digits</code>	Specifies which digits to forward for voice calls. This command is executed in dial-peer configuration mode.
<code>port port-number</code>	Configures the port for this dial peer. This command is executed in dial-peer configuration mode.
<code>preference 0-9</code>	Specifies the preferred order of a dial peer within a hunt group. This command is executed in dial-peer configuration mode.
<code>show call active voice</code>	Displays information on active calls. This command is executed in user mode.
<code>show dial-peer voice (tag) (summary)</code>	Displays dial-peer configuration information. This command is executed in user mode. The summary option is available in privileged mode only.
<code>show dialplan number number</code>	Displays which dial peer is matched when a particular telephone number is dialed. This command is executed in privileged mode.
<code>show voice call summary</code>	Displays summary information on active calls. This command is executed in user mode.

Job Aids

These job aids are available to help you complete the lab activity.

Dial Plan Conventions

As with IP addresses, the dial plan convention allows a student to anticipate the number of any telephone in the classroom. Again, for convenience, a table has been provided. The highlights of the strategy include those listed here:

- The classroom uses a four-digit dial plan.
- The first digit identifies the pod number (1 to 6).
- The second and third digits identify the device (PSTN=00, R1=10, PBX1=15, R2=20, PBX2=25).
- The fourth digit identifies the telephone.

Classroom Dial Plan

Pod Number		1	2	3	4	5	6
R1		1101	2101	3101	4101	5101	6101
		1102	2102	3102	4102	5102	6102
PBX1		1151	2151	3151	4151	5151	6151
R2		1201	2201	3201	4201	5201	6201
		1202	2202	3202	4202	5202	6202
PBX2		1251	2251	3251	4251	5251	6251
PSTN	Port 1	555-1001	555-2001	555-3001	555-4001	555-5001	555-6001
	Port 2	555-1002	555-2002	555-3002	555-4002	555-5002	555-6002
	Port 3	555-1003	555-2003	555-3003	555-4003	555-5003	555-6003

Task 1: Establish Voice Calls Between Locally Terminated Telephones

In this task, you will configure dial peers so that you can make calls between two telephones connected to your voice-enabled router.

Activity Procedure

Complete these steps:

- Step 1** Using the Classroom Dial Plan table in the Job Aids section, verify the telephone numbers that you will use for your local telephones. Note these numbers here.

1st telephone _____ 2nd telephone _____

- Step 2** Configure dial peers to enable calls between these two locally terminated telephones in both directions. Place calls in both directions to test the configuration.
- Step 3** Use the appropriate commands to view your newly configured dial peers.
- Step 4** Place a call between telephones and leave them both off hook. Use appropriate commands to view your active call. Find this information:
- How many and what type of call legs were created? _____
- Which codec is being used for this call? _____
- What is the original calling number? _____ called number? _____
- Step 5** Use the **debug** command to see digits being collected by the voice port. Once debugging is turned on, place a call between telephones to view the digit collection.
- Step 6** Verify and experiment with previously configured voice port parameters such as **cptone** and **ring cadence**. Listen to the distinctive rings you have configured. You may have to shut down and restart the voice port for the new ring cadence to take effect.

Activity Verification

You have completed this task when you attain this result:

- You have made calls between your locally terminated telephones in both directions.

Task 2: Forward Calls to the PSTN

In this task, you will configure the appropriate ports and dial peers to place calls to the PSTN. Initially, this will be done with two-stage dialing, which means that you will hear two dial tones while placing the call. The first dial tone will be from your local router, and the second will be from the PSTN. Once this configuration is verified, you will change your configuration to place the call using one-stage dialing (only the local dial tone is heard), forwarding digits to the PSTN to automatically place the call.

Activity Procedure

Complete these steps:

- Step 1** Connect the PSTN device to each pod routers using RJ-11 cables. Connect a single telephone to the PSTN device. Answer these questions:
- a) Which voice port type did you connect to the PSTN? _____
 - b) What is the port number? _____
 - c) What is the telephone number of your PSTN port? _____
 - d) What is the telephone number of the PSTN port of your partner? _____
 - e) What is the telephone number of the PSTN-connected telephone?

- Step 2** A requirement is to dial “9” to access the PSTN. Configure dial peers to allow access to the PSTN by dialing only “9” and then dialing the PSTN phone after the second dial tone is heard. Verify calls in both directions. Remember, at this point, you will hear two dial tones while placing the call.

Step 3 Edit the dial peer you just created to ring the PSTN phone and forward all appropriate digits to the PSTN so that only the local dial tone is heard. What is the default digit forwarding behavior on a POTS dial peer?

Step 4 What command did you use to forward digits to the PSTN? _____

Step 5 What other method could you have used? _____

Activity Verification

You have completed this task when you obtain this result:

- You have placed calls to the PSTN telephone with both one-stage and two-stage dialing.

Task 3: Hunt Groups

In this task, you will configure a hunt group to send calls to both of your locally terminated telephones using the same number.

Activity Procedure

Complete these steps:

Step 1 For the hunt group number, you will use the same first three digits as your telephones are now configured for. The fourth digit will be 9. For example, if your telephone numbers are 1101 and 1102, you will use 1109 as the hunt group number. Write your hunt group number.

Hunt group number _____

Step 2 Ensure that both telephones are still connected to your router voice ports.

Step 3 Configure additional dial peers for your local FXS ports to reach both voice ports using the same new hunt group number for each dial peer. Do not edit existing dial peers for this activity, because they will be needed for future labs. This means that you will have two new dial peers, each for the same hunt group number (such as 1109), assigned to each of your FXS ports. You will also have the original dial peers configured from Task 1.

Step 4 To properly test the hunt behavior between your two phones, you will use the PSTN telephone. To reach the hunt group number from the PSTN phone, dial the seven-digit PSTN number of the FXO port that attaches to your router. At the secondary dial tone, dial your hunt group number. Repeat this many times, taking note of any patterns as to how calls are allocated to each telephone. The default behavior at this point will be random choosing of a port. However, to demonstrate this randomness with only two telephones, you may have to make a number of calls.

Step 5 One way to control the order of hunting is through the use of the **preference** command. What is the default setting for preference on a dial peer? _____

What command did you use to verify the setting? _____

Change the preference on one of your hunt dial peers to 1. Which setting is preferred, the 0 or 1 setting? _____

Test the hunt group again by calling several times, making note of which telephone rings first. Is this what you expected? Now take the preferred telephone off hook and dial the hunt group number again. Did the other telephone ring? _____

On the dial peer with the preference set to 0, change the preference to 2. Which telephone should always ring first? Test the hunt group again. Is the outcome what you expected? _____

Step 6 You can configure hunt behavior for all dial peers globally with the **dial-peer hunt** command. Before changing this setting, find out what the default setting is and note it here.

Default dial-peer hunt setting _____

What command did you use to view this? _____

Configure the **dial-peer hunt** setting to 7. How do you expect your hunt group to choose which telephone to ring now? Test the hunt group again. Is the outcome what you expected? _____

Step 7 Delete the dial peers you created for the hunt groups.

Activity Verification

You have completed this task when you attain this result:

- You can control your hunt group behavior and explain how each command works.

Task 4: Establish Calls Between Telephones Interconnected by a Digital Facility

In this task, you will configure and test dial peers to place calls to your PBX-attached telephone.

Activity Procedure

Complete these steps:

Step 1 Move one of your telephones and plug it into the lowest numbered port of your PBX device. Because the PBX device is preconfigured with the dial plan for the classroom lab, test the PBX outbound calling functionality by calling from the PBX-attached telephone to the router-attached telephone. This should work with the configuration that is in place.

Step 2 Configure dial-peer functionality on your voice-enabled router to place a call to the PBX-attached telephone.

What is the telephone number of your PBX-attached telephone? _____

What is the voice port number that you will use in this dial peer? _____

Step 3 Now that the number of dial peers is growing, check which dial peer will be matched when dialing your PBX-attached telephone number using a **show** command.

Step 4 Test the configuration by calling from your router-attached telephone to your PBX-attached telephone. Does the call go through? If not, check which digits are being forwarded to the PBX. Correct the problem and test again. If digit forwarding is correct, check the configuration of the DS0 group from Lab 4.1 or ask your instructor for assistance.

Step 5 Save your configuration.

Activity Verification

You have completed this task when you attain this result:

- You have called in both directions between the PBX-attached telephone and the router-attached telephone.

Lab 2-4: Configuring Special-Purpose Connections

Complete this lab activity to practice what you learned in the related module.

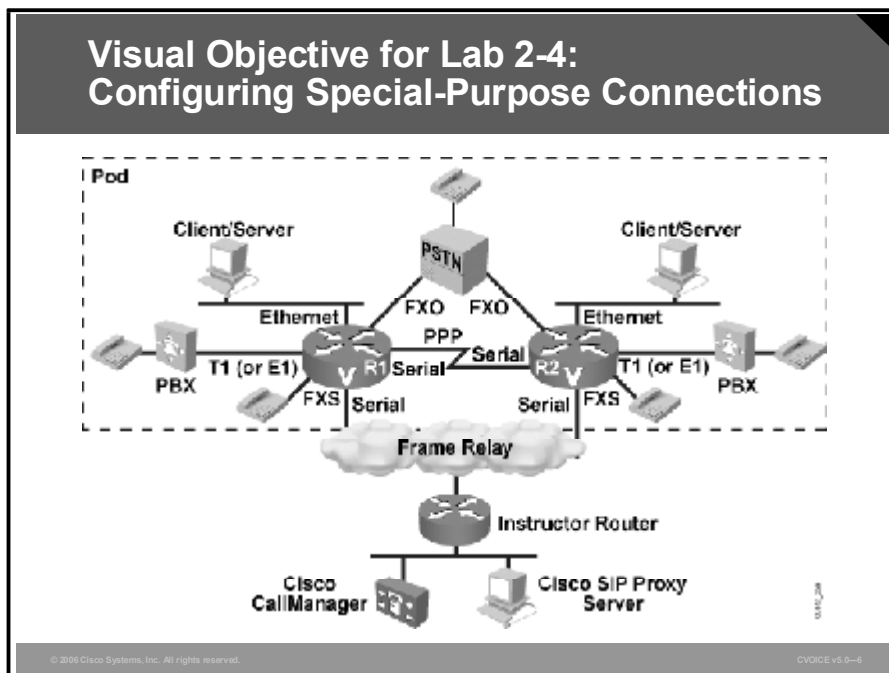
Activity Objective

In this activity, you will explore different connection types and their uses. After completing this activity, you will be able to meet these objectives:

- Simulate auto attendant functions through use of PLAR and PLAR OPX
- Create a tie-line connection for calls between two PBXs
- Use appropriate **show** and **debug** commands to monitor and troubleshoot the connections

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:

- No new resources are required.

Command List

The table describes the commands that are used in this activity.

Connection Commands

Command	Description
<code>connection plar opx string</code>	Specifies a PLAR OPX connection. This command is executed in voice-port configuration mode.
<code>connection plar string</code>	Specifies a PLAR connection. This command is executed in voice-port configuration mode.
<code>connection tie-line string</code>	Specifies a tie-line connection. This command is executed in voice-port configuration mode.

Job Aids

There are no job aids for this lab activity.

Task 1: Connecting to PLAR and PLAR OPX

By default, when a call comes into an FXO port, the router presents a dial tone after going off hook to answer the call. At times, this default behavior may not be desirable. In this task, you will configure the voice port to simulate an auto attendant function.

Activity Procedure

Complete these steps:

Caution Do *not* save your configuration during this lab. You will be asked to reload the router at the end of the lab to revert back to the last lab configuration.

- Step 1** For this task, you will use the PSTN telephone to dial into the router FXO port. You want the FXO port to automatically direct the incoming call to your router FXS telephone, thereby simulating auto attendant. Simulate the auto attendant function by configuring PLAR on the FXO port of your voice-enabled router. Direct all calls coming into the FXO port to the telephone connected to your FXS port on the same router.
- Step 2** Test the functionality by placing a call from the PSTN-attached telephone to your router-attached telephone. Do you hear one or two dial tones? Place another call. Listen carefully to the ringback tone. You should hear an initial ringback from the PSTN, followed by a secondary ringback from the FXS port as it is ringing the telephone. From the perspective of the PSTN, the call is complete when its ringing is answered and billing has started, even though the FXS port is still ringing.
- Step 3** Change the PLAR configuration to **plar-opx**, pointing it to the same telephone number as in Step 2.

- Step 4** Test the functionality by placing another call from the PSTN-attached telephone to the router-attached telephone. Is the ringback tone different than in Step 2? Did you hear a second ringback tone? _____

Activity Verification

You have completed this task when you attain these results:

- You have placed a call to the FXO port of your router from the PSTN-attached telephone and, without further dialing, connected to the router-attached telephone.
- You can explain the difference between PLAR and PLAR OPX.

Task 2: Connection Tie-Line

In Task 1, you configured a PLAR connection and saw that the configuration allowed for calls to a single specific number without access to a dial tone. Traditionally, tie-lines connect two PBXs together when a user at one site needs to connect to any number of users at the other site. Configuring tie-lines gives you the capability to call multiple numbers at the remote site by dialing the number directly upon receiving dial tone.

Activity Procedure

Complete these steps:

Note Do *not* save your configuration in this lab. You will be asked to reload the router at the end of the lab to revert to the previous lab configuration.

Step 1 Configure tie-line functionality on your digital voice port. For the string entry, the odd-numbered routers will use the digit 7 to reach the even-numbered PBX, and the even-numbered routers will use the digit 8 to reach the odd-numbered PBX. This code ties all calls coming into the digital voice port from your PBX to a dial peer that will point the call across the network to the remote site and vice versa. Although you only dial a four-digit number to reach the remote site, the router will be processing a five-digit number because it will automatically prepend the code digit to your four-digit number.

Step 2 Now you need to configure a VoIP dial peer to point the call across the network toward the PBX of your partner. Because there is no loopback address, you can send the call to any valid address on the router of your partner.

Write the IP address of your partner here. _____

Ping the router of your partner to ensure connectivity.

Remember, the router is processing your code digit plus the four digits you will dial for a five-digit dialing string.

What four-digit number will you dial to reach the PBX-attached telephone of your partner? _____

What five-digit number will the router process to connect to the PBX-attached telephone of your partner? _____

Step 3 To complete the tie-line connection across the IP network, you will have to enter the this VoIP dial-peer command:

```
router(config)# dial-peer voice tag voip
```

```
router(config-dial-peer)# destination-pattern string  
(Use the five digits noted in Step 2.)
```

```
router(config-dial-peer)# session target ipv4:x.x.x.x  
(Use the IP address from Step 2.)
```

Step 4 As in the last task, remember that your partner will be calling your PBX-attached telephone as well. The router of your partner will be passing a five-digit string to your router to complete the call to your PBX.

What five-digit string will the partner router be passing to your router for calls destined for your PBX telephone? _____

Configure a POTS dial peer to terminate the five-digit string as it comes in from the partner router and to forward only the four required digits to your PBX via the digital voice port.

Step 5 Coordinate with your partner to ensure that all tasks are complete before testing. Test the configuration by placing calls between the PBX-attached telephones in both directions. Use **show** and **debug** commands to view the processing of the call.

Step 6 Reload the router to revert back to your previous configuration. When you are asked if you wish to save your configuration, enter **no**.

Activity Verification

You have completed this task when you attain these results:

- You have configured and verified tie-line connections between PBXs.
- You have placed calls in both directions between PBX-attached telephones.

Lab 2-5: Configuring Basic VoIP Network Connections

Complete this lab activity to practice what you learned in the related module.

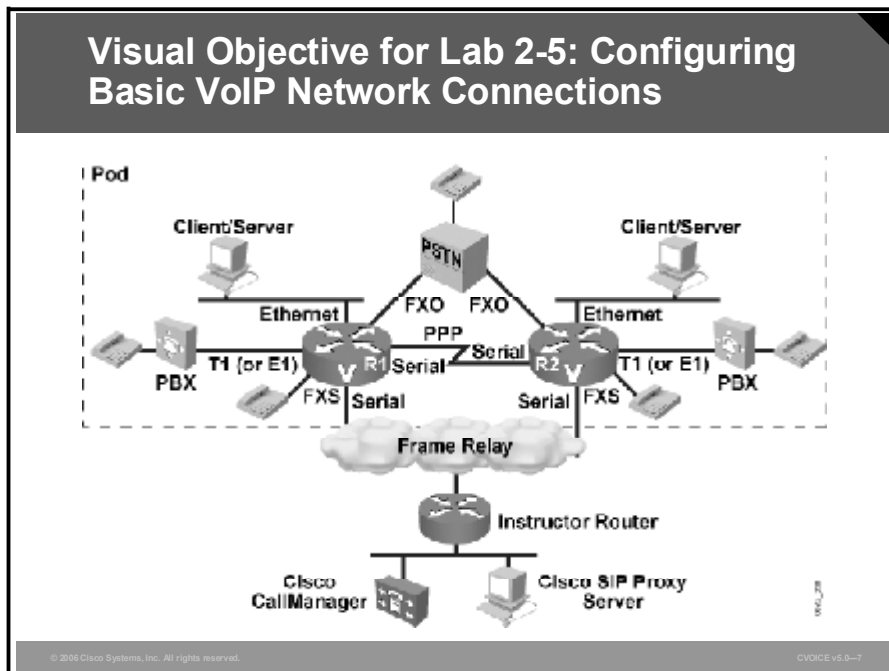
Activity Objective

In this activity, you will establish basic VoIP connectivity between telephones in your pod. You will also investigate the use of appropriate VoIP dial-peer parameters. After completing this activity, you will be able to meet these objectives:

- Configure VoIP connections
- Describe how dial-peer matching occurs
- Describe and configure proper use of dial-peer codec parameters
- Verify basic call setup through **debug** commands
- Use appropriate **show** and **debug** commands to monitor and troubleshoot the connections

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:

- No new resources are required.

Command List

The table describes the commands that are used in this activity.

VoIP Commands

Command	Description
<code>codec codec-name</code>	Specifies which codec is to be used for calls matching this dial peer. This command is executed in dial-peer configuration mode.
<code>codec preference 1-14 codec-name</code>	Configures one entry in the codec list under the voice class codec command. Repeat this command as many times as you need to specify codecs in this list. This command is executed in voice class configuration mode.
<code>debug voip ccapi inout</code>	Displays real-time call control processing and call leg information. This command is executed in privileged mode.
<code>default parameter</code>	Sets the specified parameter back to its default setting. For example, default codec will set the dial peer to use the default codec for that device. This command can be executed in various configuration modes.
<code>dial-peer voice tag voip</code>	Enters dial-peer configuration mode and specifies VoIP. This command is executed in global configuration mode.
<code>frame relay ip rtp header-compression</code>	Enables RTP header compression on a Frame Relay interface. This command is executed in interface configuration mode.
<code>ip rtp header- compression</code>	Enables RTP header compression on an interface. This command is executed in interface configuration mode.
<code>session target ipv4:x.x.x.x</code>	Specifies the destination IP address for the gateway terminating a VoIP call. This command is executed in dial-peer configuration mode.
<code>show voice dsp</code>	Displays DSP usage. This command is executed in user mode.
<code>show ip rtp header- compression</code>	Displays statistics relating to RTP header compression. This command is executed in user mode.
<code>voice class codec tag</code>	Enters voice class codec configuration mode. This command is executed in global configuration mode.
<code>voice-class codec tag</code>	Applies a predefined codec list to a dial peer. The tag must match the tag of the defined codec class. This command is executed in dial-peer configuration mode.

Job Aid

This job aid is available to help you complete the lab activity:

- Understanding **debug voip ccapi inout** command output

Task 1: VoIP Dial Peers

In this task, you will start by configuring basic VoIP dial peers using the default parameters to process the call. You will verify configuration by placing calls across the IP network to the telephones of your partner.

Activity Procedure

Complete these steps:

Step 1 Move the PBX-attached telephone to the voice router. At this point, you should have two telephones attached to the two FXS ports on your voice router.

Step 2 Configure VoIP dial peers to reach both of the router-attached telephones connected to the equipment belonging to your partner. In preparation, note the two telephone numbers for your partner here. Also note a valid IP address on the partner router.

Telephone numbers _____

IP address _____

Step 3 Test your configuration by placing calls to both of the partner telephones.

Step 4 Use **show** commands to verify the following:

- Which dial peer will be matched when a specific number is dialed
- Active call parameters
- What DSP resources are being used for the call

Step 5 Use **debug** commands to verify the following:

- The calling number
- The called number
- Which dial peer was matched

Activity Verification

You have completed this task when you attain this result:

- You have placed calls to both of the partner telephones.

Task 2: Codec Configuration

In this task, you will change the codec settings on your VoIP dial peers and investigate how it affects the ability to make calls. Make sure that you and your pod partner are both working on the same step. Coordinate moving through the steps and performing tests together.

Activity Procedure

Complete these steps:

Step 1 Use **show** commands to verify the default codec setting and note it here.

Default codec _____

Step 2 Change the codec on the R1 VoIP dial peer pointing to R2. Set the codec to g723r53.

Step 3 Both R1 and R2 should verify whether the call was successful, and if so, which codec was used.

Was the call successful? _____ Codec used _____

Step 4 Change the codec on the R2 VoIP dial peer pointing to R1 to match the R1 codec.

Step 5 Verify whether the codec was successful, and if so, which codec was used.

Was the call successful? _____ Codec used _____

Step 6 Change the codec setting back to default.

Activity Verification

You have completed this task when you attain this result:

- You have successfully configured the codec setting for VoIP calls.

Task 3: Effects of Bandwidth Requirements and Header Compression

In this task, you will investigate the effects of passing voice over low bandwidth links and the tools available to improve voice quality on those links.

Activity Procedure

Complete these steps:

Step 1 Using the bandwidth requirement concepts, determine the required bandwidth for a G.711 call using a 160-byte payload and without header compression on these links.

PPP link _____

Frame Relay link _____

Step 2 Change the codec on both R1 and R2 to g711ulaw. Place a call from one router-connected telephone to the other router-connected telephone over the IP network. Is the quality acceptable? If not, why not? _____

Step 3 Enable RTP header compression on your PPP and Frame Relay interfaces on both routers in your pod.

- Step 4** What command did you use on the PPP link? _____
- Step 5** What command did you use on the Frame Relay link? _____
- Step 6** Test the voice quality. Has the quality improved? Why or why not? Is it acceptable?
- Step 7** Change the codec on both R1 and R2 back to the default setting. What command did you use to reset to the default? _____

Activity Verification

You have completed this task when you attain this result:

- You can explain how and when to use RTP header compression.

Task 4: Configuring Codec Negotiation

As you saw in the previous labs, configuring a specific codec at the dial-peer level restricts that dial peer to responding with only a single codec choice during negotiation. At times, it is desirable to respond with a list of codecs to match the incoming call. For example, when a call is coming from the LAN segment, it may negotiate a G.711 codec for better voice quality because there is enough bandwidth to carry it. For a call coming into the router from a WAN segment, you will want to match a codec for compressed voice. For a single dial peer to match more than one codec, you must configure a list of codecs to negotiate.

Activity Procedure

Complete these steps:

- Step 1** Define a codec preference list. On R1, select g711ulaw as the first choice and g729r8 as the second choice. On R2, select g729r8 as the first choice and g711ulaw as the second choice.
- Step 2** Apply the codec list to the VoIP dial peer pointing to the IP address of your partner.
- Step 3** Test calls in both directions. Use **show** commands to determine the order of preference for codec selection. Discuss the results with your partner.
- Step 4** Remove the codec list and its application in the dial peer.
- Step 5** Save your configuration.

Activity Verification

You have completed this task when you attain this result:

- You can explain how and when to configure codec negotiation parameters.

Lab 3-1: Configuring VoIP with H.323

Complete this lab activity to practice what you learned in the related module.

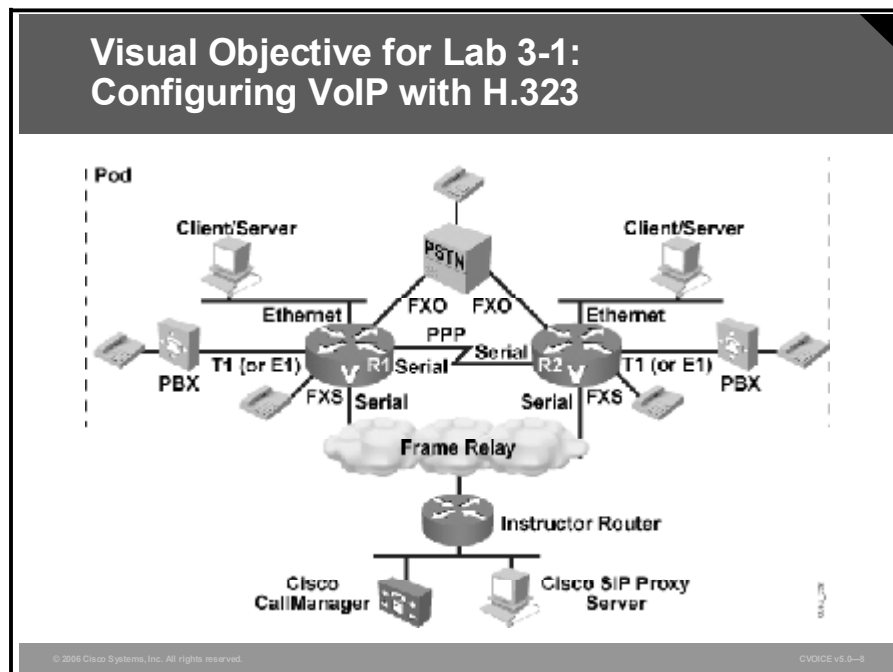
Activity Objective

You need to be able to call all other router-attached telephones in the classroom. Because there are several sets of routers and numerous telephones in the classroom lab, you do not want to manually enter dial peers for all possible telephones. In this activity, you will implement a scalable VoIP environment using H.323 gatekeepers. You will experiment with a single-zone, single-gatekeeper environment and a multizone environment including multiple gatekeepers. After completing this activity, you will be able to meet these objectives:

- Configure single-zone and multizone H.323 gatekeeper environments for VoIP scalability
- Use **debug** and **show** commands to monitor the status and progress of call setup procedures in an H.323 environment

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:

- Instructor router with gatekeeper functionality enabled

Command List

The table describes the commands that are used in this activity.

H.323 Commands

Command	Description
<code>debug cch323 h225</code>	Traces the state transition of the H.225 state machine based on the processed event. This command is executed in privileged mode.
<code>debug gatekeeper server</code>	Traces all the message exchanges between the Cisco IOS gatekeeper and the external applications. This command is executed in privileged mode.
<code>gatekeeper</code>	Enables gatekeeper functionality. This command is executed in global configuration mode.
<code>gateway</code>	Enables gateway configuration. This command is executed in global configuration mode.
<code>h323-gateway voip interface</code>	Specifies that the IP address of this interface will be used to register with the gatekeeper. This command is executed in interface configuration mode.
<code>h323-gateway voip id gatekeeper-id ipaddr gatekeeper-ip-addr</code>	Defines the name and location of the gatekeeper for this gateway. This command is executed in interface configuration mode.
<code>h323-gateway voip h323-id</code>	Defines the name that will be used to identify this gateway to the gatekeeper. This command is executed in interface configuration mode.
<code>session target ras</code>	Specifies that the RAS protocol is being used to determine the IP address of the session target. This command is executed in dial-peer configuration mode.
<code>show gatekeeper option</code>	Displays various parameters and statuses for a gatekeeper. This command is executed in user mode on the gatekeeper.
<code>show gateway</code>	Shows if the gateway is connected to the gatekeeper. This command is executed in user mode on the gateway.
<code>zone local remote</code>	Statically specifies a local or remote zone. The parameters include gatekeeper name, domain name, and IP address. This command is executed in config-gk configuration mode.
<code>zone prefix</code>	Specifies which group of telephone numbers is reachable via a specific gatekeeper. The prefix typically contains wildcards for number summarization. This command is executed in config-gk configuration mode.

Job Aid

This job aid is available to help you complete the lab activity:

- The instructor router gateway is gk; the IP address of the instructor router is 192.168.100.1.

Task 1: Single-Zone Environment

In this task, you will configure your router to be a gateway that registers with a gatekeeper. This is a single-zone configuration, because all of the voice-enabled routers will register to a single gatekeeper.

Activity Procedure

Complete these steps:

- Step 1** Enable **debug** to see the interactions between H.323 components once gatekeeper support has been enabled. Ensure that you can reach the gatekeeper by pinging 192.168.100.1.
- Step 2** Using the bulleted items here, configure your router as an H.323 gateway. Initially, all routers will use the instructor router as their gatekeeper. The IP address of the instructor router is 192.168.100.1. Analyze the **debug** command output to observe the interactions between your router and the gatekeeper. These tasks are necessary to register with a gatekeeper:
- Configure your router to be a gateway.
 - Specify which interface IP address will be used to register with the gatekeeper and also specify the identity of the gatekeeper. Use your Ethernet interface for gateway configuration.
 - Specify an H.323 ID for your gateway by combining “gw” with your pod and router number. For example, if you were pod 5, router 2, your H.323 ID would be gwP5R2.
 - Use the **show gateway** command on your router to verify that you have registered with the gatekeeper.

What is the gatekeeper name you have registered with? _____

Under the CLI alias list, which numbers register with the gatekeeper? _____

- Step 3** Connect to the instructor router and use variations of the **show gatekeeper** command to verify that your router is registered and that your router has registered the destination patterns from your POTS dial peers.

What IP address is registered to be used for calls to your device? _____

What port number is being used for call signaling? _____

What is the H.323 ID of your router? _____

What zone is your gateway part of? _____

- Step 4** Create a dial peer to use RAS for all calls to destinations outside your pod. Be creative when creating this dial peer.

Step 5 Establish a voice call to a telephone in another pod. Use the **show call active voice** command to provide the information that follows:

How many and what type of call legs are established? _____

Calling number _____

Called number _____

Remote IP address _____

Remote UDP port _____

Step 6 Place another call to a telephone outside your own pod. Use the **debug cch323 h225** command to provide the information that follows:

What is the source address of the call? _____

What is the destination address of the call? _____

Note Do not proceed to Task 2 until all the pods have completed Task 1 and the instructor tells you to proceed.

Activity Verification

You have completed this task when you attain these results:

- You have configured and verified that your gateway has registered with a gatekeeper.
- You can call all of the other telephones in the classroom.

Task 2: Multizone Environment

In this task, you will configure your voice-enabled router to be both a gateway and a gatekeeper. The gateway function of your router will be configured to register internally with the gatekeeper function of your router. Because all the other routers are also configuring themselves to be gatekeepers, this will be a multizone configuration.

Activity Procedure

Complete these steps:

- Step 1** You already have VoIP dial peers to the telephones belonging to your partner in your own pod by way of specific dial peers. Leaving this functionality in place, you will now expand reachability to other pods by setting up gatekeeper capabilities on your router and configuring your router to know about other gatekeepers outside your pod. Using the bulleted items here, enable gatekeeper functionality on your router. In your gatekeeper configuration, include the routers in the other pods as remote zones (gatekeepers), but do not include the other router in your pod as a remote zone. To enable gatekeeper functionality, perform these tasks:
- Enable gatekeeper functionality.
 - Define your local zone information. For your zone name, use “gk” plus your pod and router numbers. For example, if you are in pod 3, router 1, your zone name will be gkP3R1. The domain name is cisco.com. Use your Ethernet IP address for the RAS address. Make sure that your gatekeeper is not in shutdown state.
 - Define all remote zones using the same naming and addressing convention as in the Task 1. Do not include the other router in your pod as a remote zone. Configure the **zone prefixes** command for all remote zones only.
 - Change the H.323 gateway configuration on your router to point to your own router as the gatekeeper. Ensure that you use the ID and IP address set up in the previous tasks. This configuration connects the gateway process in your router. The gateway process in your router then sets up telephone calls to the gatekeeper that knows about all the other gatekeepers in the classroom.
 - Establish calls to other pods and use **show** and **debug** commands to observe the interactions between H.323 components.
- Step 2** Save your configuration.

Activity Verification

You have completed this task when you attain these results:

- You have configured and verified that your gateway has registered with a gatekeeper.
- You have configured and verified gatekeeper functionality on your router.
- You can call all of the other telephones in the classroom.

Lab 3-2: Configuring VoIP with SIP

Complete this lab activity to practice what you learned in the related module.

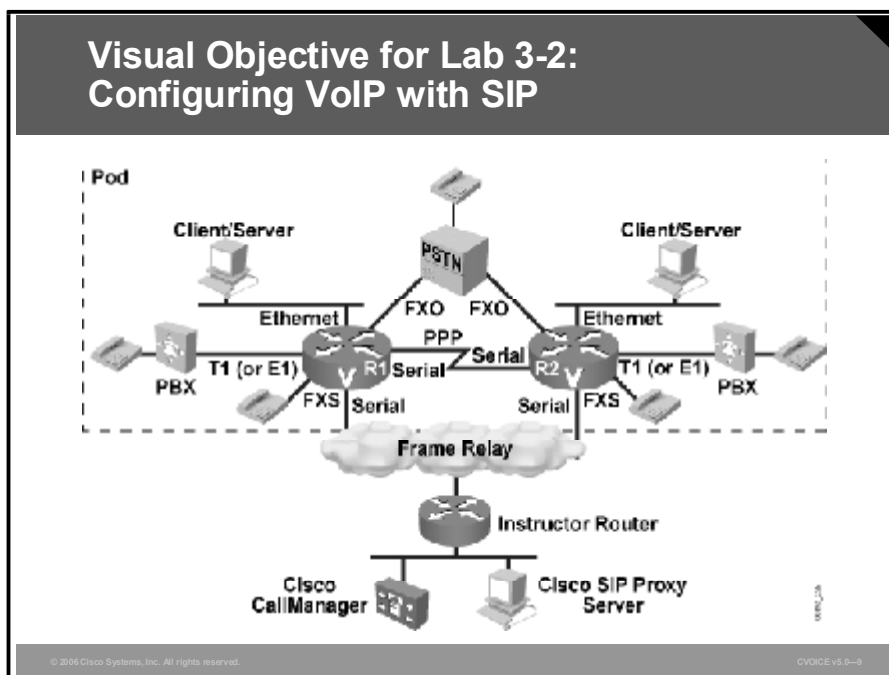
Activity Objective

In this activity, you will use SIP direct procedures (UA to UA) to establish VoIP calls. After completing this activity, you will be able to meet this objective:

- Configure dial peers to use SIP call control procedures to set up VoIP calls

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:

- Standard equipment listed for CVOICE labs

Command List

The table describes the commands that are used in this activity.

SIP Commands

Command	Description
<code>debug ccsip options</code>	Displays various real-time SIP call information. This command is executed in privileged mode.
<code>session protocol sipv2</code>	Specifies that the VoIP dial peer should use SIP call control when processing the call. This command is executed in dial-peer configuration mode.
<code>session target sip-server</code>	Specifies the use of the proxy server. This command is executed in dial-peer configuration mode.
<code>show sip-ua options</code>	Displays various parameters for SIP. This command is executed in privileged mode.
<code>sip-ua</code>	Enters SIP UA configuration mode. This command is executed in global configuration mode.

Job Aids

There are no job aids for this lab activity.

Task 1: Configuring for SIP

In this task, you will configure your router to initiate calls with the router of your partner using SIP. For this activity, you will use SIP direct—UA to UA.

Activity Procedure

Complete these steps:

Note Do *not* save your configuration in this lab. You will be asked to reload the router at the end of the lab to revert to the previous lab configuration.

- Step 1** Modify the existing VoIP dial peers that point to the telephones belonging to your partner to use direct unnumbered acknowledgment (UA to UA) SIP call control procedures when establishing voice calls. For direct calls, the IP address in the **session target** command will be a valid address of the partner router.
- Step 2** Use the **show call active voice** command to verify that you now have SIP call legs when placing a call to a partner telephone.
- Step 3** Enable SIP debugging and place a call between your telephone and a partner telephone. Observe the call setup, capabilities negotiation, and assignment of ports for the call.

- Step 4** Investigate the status of SIP with variations of the **show sip-ua** command.
- Step 5** Do not save your configuration at this time. You will be asked to reload the router after the next lab.

Activity Verification

You have completed this task when you attain this result:

- You have established voice calls between telephones connected to your routers by way of direct SIP call control procedures.

Lab 3-3: Configuring VoIP with MGCP

Complete this lab activity to practice what you learned in the related module.

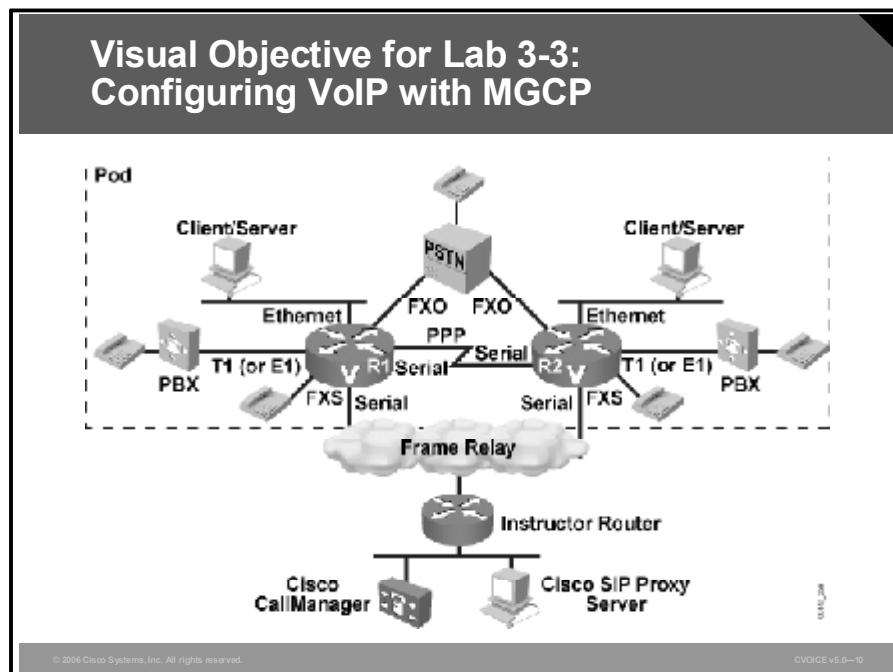
Activity Objective

In this activity, you will use a call agent to establish voice calls between telephones connected to MGCP residential gateways. After completing this activity, you will be able to meet these objectives:

- Configure your routers as MGCP residential gateways and have the routers use an MGCP call agent to establish voice calls between them
- Use **debug** commands to analyze the interactions between MGCP gateways and a call agent
- Use **show** commands to view the status of MGCP endpoints, connections, and calls

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:

- MGCP call agent resident on the instructor LAN

Command List

The table describes the commands that are used in this activity.

MGCP Commands

Command	Description
<code>application mgcpapp</code>	Enables MGCP for the voice port configured in this dial peer. This command is executed in dial-peer configuration mode. Please note that the format of this command may change based on the version of Cisco IOS software.
<code>ccm-manager mgcp</code>	Enables support for Cisco CallManager MGCP. This command is executed in global configuration mode.
<code>debug ccm-manager options</code>	Displays real-time Cisco CallManager MGCP information. This command is executed in privileged mode.
<code>debug mgcp options</code>	Displays real-time MGCP call information. This command is executed in privileged mode.
<code>mgcp</code>	Enables MGCP functionality on the router. This command is executed in global configuration mode.
<code>mgcp call-agent ip-address</code>	Specifies the MGCP call agent IP address. This command is executed in global configuration mode.
<code>show call application voice summary</code>	Displays a list of available applications. This command is executed in user mode.
<code>show ccm-manager</code>	Displays Cisco CallManager MGCP information. This command is executed in user mode.
<code>debug ccm-manager options</code>	Displays real-time Cisco CallManager MGCP information. This command is executed in privileged mode.

Job Aid

This job aid is available to help you complete the lab activity:

- The MGCP call agent IP address is 192.168.100.100.

Task 1: MGCP Calls

In this task, you will configure your router to use the MGCP protocol for calls throughout the classroom.

Activity Procedure

Complete these steps:

Note	Do <i>not</i> save your configuration in this lab. You will be asked to reload the router at the end of the lab to revert to the previous lab configuration.
-------------	--

Step 1	Ensure that you can reach the MGCP call agent by pinging IP address 192.168.100.100. Inform the instructor if you are unable to reach the MGCP call agent.
Step 2	Enable MGCP on the routers in your pod by specifying MGCP and configuring the IP address of the call agent.
Step 3	On your router, modify the POTS dial peers defining your two telephones by removing the destination pattern and entering the application mgcpapp command. (The format of this command may change based on the version of Cisco IOS software.)
Step 4	Use show commands to verify that the gateway is registered with the Cisco CallManager.
Step 5	Enable debug and establish a call between the telephones connected to your routers. Analyze the debug command output, looking for the interactions between your router and the call agent and between your router and the destination router.
Step 6	Investigate the status of MGCP with variations of the show mgcp command.
Step 7	Reload the router. Make sure that you respond “no” when asked if you want to save your configuration.

Activity Verification

You have completed this task when you attain this result:

- You have established voice calls between the telephones connected to your routers by way of MGCP.

Lab 4-1: Implementing Cisco AutoQoS

Complete this lab activity to practice what you learned in the related module.

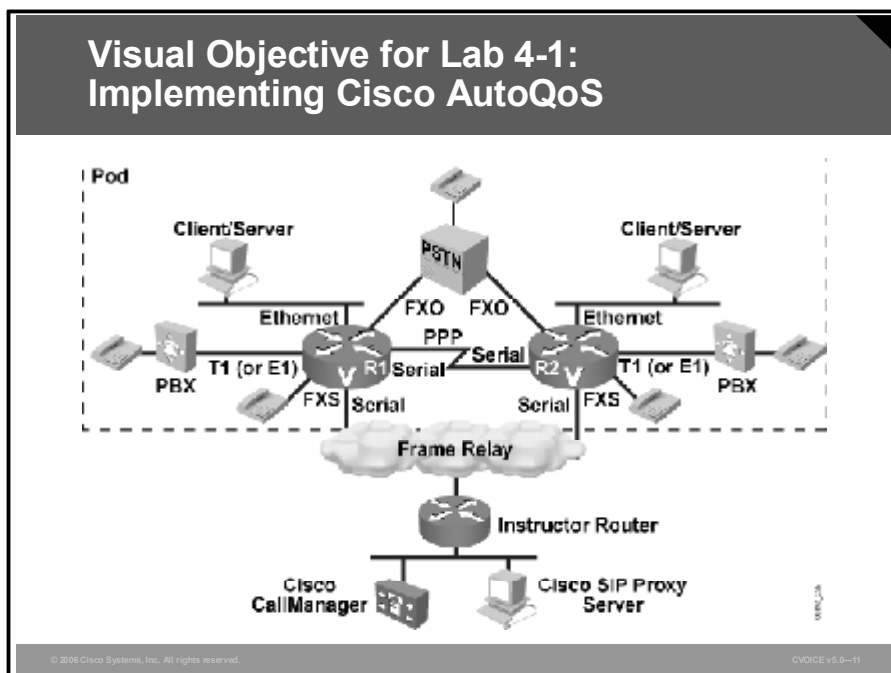
Activity Objective

In this activity, you will observe the incremental and combined effects of applying QoS concepts to improve voice quality end to end. After completing this activity, you will be able to meet these objectives:

- Implement quality improvements on low-speed links with QoS features such as fragmentation, interleaving, and Frame Relay traffic shaping
- Implement features such as voice packet marking (tagging) and queuing to improve voice quality end to end
- Confirm, by testing, that the QoS features contribute to overall improvements in voice quality

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:

- No new resources are required.

Command List

The table describes the commands that are used in this activity.

QoS Commands

Command	Description
auto qos voip	Enables Cisco AutoQoS configuration for interfaces. This command is entered in interface configuration mode, except Frame Relay, which requires subinterface configuration mode.
bandwidth <i>bandwidth (Kbps)</i>	Sets the correct bandwidth on the physical interface; must be set for correct fragment sizes to be calculated. This command is executed in interface configuration mode.
class <i>map-class-name</i>	Applies the Frame Relay map class that was created previously. This command is executed in DLCI configuration mode.
class-map <i>name</i>	Creates a class map and enters class map configuration mode. This command is executed in global configuration mode.
class <i>name</i>	Associates the previously created class map to this policy. Ensure that the same name is used as when you created the class map. This command is executed in policy map configuration mode.
clear frame-relay inarp	Clears ghost Frame Relay Inverse Address Resolution Protocol (ARP) associations. This command is executed in privileged mode.
encapsulation ppp	Enables PPP encapsulation. Configure in both serial and multilink interfaces.
fair-queue	Enables WFQ on the interface. This command is executed in MP interface configuration mode.
frame-relay bc <i>value</i>	Specifies the committed burst value. This value should be 1/100 of the CIR for a 10-ms maximum burst delay. This command is executed in map class configuration mode.
frame-relay cir <i>value</i>	Specifies the CIR of the Frame Relay link. This command is executed in map class configuration mode.
frame-relay fair-queue	Enables WFQ for the interface. This command is executed in map class configuration mode.
frame-relay fragment <i>fragment-size-in-bytes</i>	Specifies the fragment size for frames. Fragment size should be set to accommodate a 10-ms delay in queue. Calculate this based on the link speed. This command is executed in map class configuration mode.
frame-relay interface-dlci <i>dlci-number</i>	Enables DLCI configuration mode for a specific DLCI. This command is executed in interface configuration mode.

Command	Description
frame-relay traffic-shaping	Enables Frame Relay traffic shaping on the interface. This command is executed in interface configuration mode.
interface multilink <i>interface-no</i>	Creates an MP interface and enters multilink interface configuration mode. This command is executed in global configuration mode.
interface interface-type interface-number <i>subinterface-number</i> point-to-point	Creates a subinterface on the main interface. This command is executed in interface configuration mode.
ip cef	Enables Cisco Express Forwarding switching on interfaces. This command is entered in global configuration mode.
ip qos dscp <i>option</i>	Specifies the DSCP for the dial peer. Use class selector 5 (cs5) to specify an IP precedence of 5. This command is executed in dial-peer configuration mode.
map-class frame-relay <i>name</i>	Creates a Frame Relay map class and enters map class configuration mode. This command is executed in global configuration mode.
match ip dscp <i>cs5</i>	Specifies that the class map should match packets marked with a precedence of 5. This command is executed in class map configuration mode.
multilink-group <i>group-no</i>	Used to link the multilink (logical) interface to the serial (physical) interface. Use the same command and group number in both interfaces to bind them together.
policy-map <i>name</i>	Creates a policy map and enters policy map configuration mode. This command is executed in global configuration mode.
ppp multilink	Enables MLP on an interface. Configure in both serial and multilink interfaces.
ppp multilink fragment delay <i>delay-max</i>	Specifies a maximum size in units of time for packet fragments on an MLP bundle. This command is executed in MP interface configuration mode.
ppp multilink interleave	Enables interleaving of packets among the fragments of larger packets on an MLP bundle. This command is executed in MP interface configuration mode.
priority <i>bandwidth</i>	Assigns the voice class traffic to the priority queue and specifies how much bandwidth to allow for that queue. This command is executed in policy map configuration mode.
service-policy <i>direction name</i>	Associates a policy map to an interface. Ensure that you use the same name as that of the policy map you created. This command is executed in interface configuration mode.
show policy-map interface <i>int-number</i>	Displays the policy applied to the interface. This command is executed in use mode.

Job Aids

There are no job aids for this lab activity.

Task 1: Enabling AutoQoS

In this task, you will configure Cisco AutoQoS on the Frame Relay interface. You will be tasked with working within your pod to accomplish voice calls with QoS enabled.

Activity Procedure

Complete these steps:

-
- | | |
|-------------|--|
| Note | Do <i>not</i> save your configuration in this lab. You will be asked to reload the router at the end of the lab to revert to the previous lab configuration. |
|-------------|--|
-
- Step 1** Enable Cisco Express Forwarding switching on the router.
- Step 2** Shut down the PPP interface that connects to the other router in your pod.
- Step 3** Using the **show frame-relay map** command, make a note of the correct DLCI number that connects to the router of your pod partner. The correct map will show the IP address of the Frame Relay interface of your partner. The DLCI number is:

- Step 4** To prepare for Cisco AutoQoS, your Frame Relay interface must be changed to a subinterface. To do this, first delete the IP address from the main Frame Relay interface. Next, go to privileged mode, and clear the Frame Relay Inverse ARP table with the command **clear frame-relay inarp**. Next, create a point-to-point subinterface on the main Frame Relay interface. Assign the IP address that you deleted from the main interface. Then, add a bandwidth statement reflecting 72 Kbps (remember that Cisco AutoQoS requires a bandwidth statement). Finally, add the **frame-relay interface-dlci** statement with the DLCI number that you noted in Step 3.
- Step 5** Be sure that all of the steps outlined in Step 4 are completed.
- Step 6** Reconfigure your dial peer that points to the partner phones so that the session target points to the IP address of their Frame Relay interface.
- Step 7** Ensure that you can ping the Frame Relay IP address of your partner. Each of you must have completed all of the steps up to this point for the ping to work correctly. If necessary, wait for the other router to get to this point.
- Step 8** Ensure that calls can be made in both directions. If not, check your dial peers. Notify your instructor if calls cannot be made.
- Step 9** Using an extended ping from one router only, send 100,000 pings at 1500 bytes each to the other router. The pings should be successful. Allow the pings to run.
- Step 10** From the router where the pings were initiated, place a call to the partner router. Test the voice quality by counting to 20 quickly. What is the quality of the call? Are there dropouts or missing audio periods? Discuss the results with your partner. Hang up the phones, abort the ping, and repeat the test in the other direction.
- Step 11** Go to configuration mode for the DLCI on the subinterface you created. In DLCI configuration mode, add the command **auto qos voip**. The router will pause for a few seconds, then return a prompt.

Step 12 Return to privileged mode and look at the running configuration.

What access list (or lists) was (or were) created?

How many classes were created in the policy map? _____

In the map class, what fragment size was configured? _____

Why? _____

What map class was assigned to the Frame Relay subinterface DLCI?

Step 13 From one router, send a continuous count of 100,000 pings at 1500 bytes each. Place a call from the router initiating the ping and check voice quality by counting to 20 quickly. Did the voice quality improve? Discuss the results with your partner, then hang up, abort the ping, and repeat the test in the other direction.

Step 14 Reload the router. Make sure that you respond “no” when asked if you want to save your configuration.

Activity Verification

You have completed this task when you attain this result:

- You have maintained voice quality while transferring data over a shared path.

Lab 4-2: Implementing CAC

Complete this lab activity to practice what you learned in the related module.

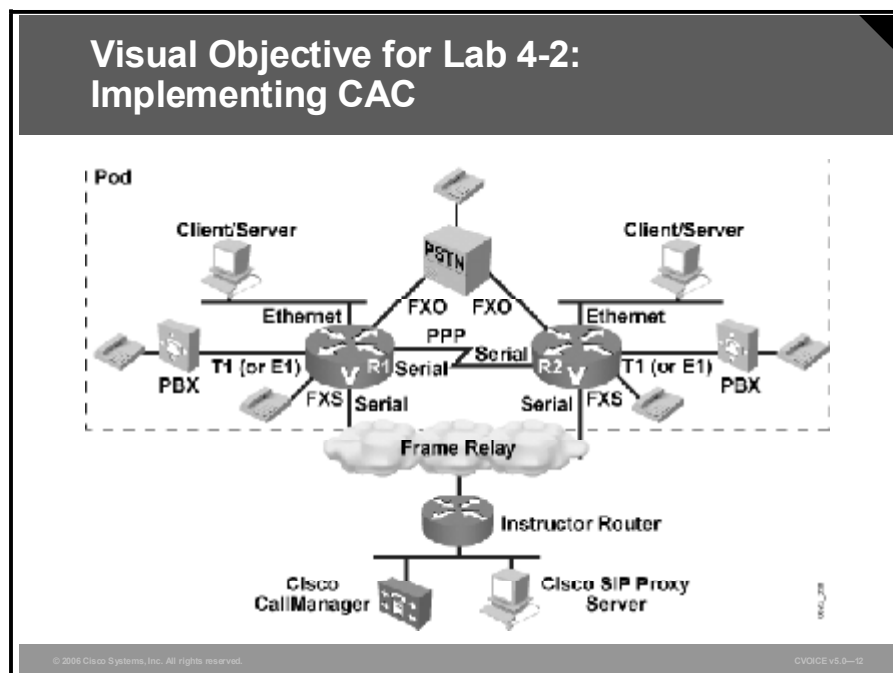
Activity Objective

In this activity, you will observe the incremental effects of applying CAC concepts to control the number of concurrent calls across the network. After completing this activity, you will be able to meet these objectives:

- Implement CAC using dial-peer configuration, RSVP, and H.323 gatekeeper configuration commands
- Use **debug** commands to view real-time CAC processing
- Confirm, by testing, that the CAC implementation limits the number of concurrent calls that can be placed to or from the configured location

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

No new resources or equipment are required to complete this activity.

Command List

The table describes the commands that are used in this activity.

CAC Commands

Command	Description
<code>max-conn</code>	Sets the maximum connections per dial peer for both inbound and outbound peer matches. This command is executed in dial-peer configuration mode.
<code>debug voice ccapi individual 6</code>	Displays debug output specifically for call control application programming interface (CCAPI) debug message 6, which is generated when a call is attempted that exceeds the configured max-conn count for the dial peer. This command is executed in privileged mode.
<code>ip rsvp bandwidth bandwidth</code>	Configures the maximum bandwidth that can be reserved by RSVP. Bandwidth is entered in kilobits per second. This command is executed in interface configuration mode.
<code>req-qos</code>	Configures the requested QoS to be used for calls matching this dial peer. This command is executed in dial-peer configuration mode.
<code>acc-qos</code>	Configures the minimally acceptable QoS to be used for calls matching this dial peer. This command is executed in dial-peer configuration mode.
<code>debug ip rsvp traffic-control</code>	Displays resource allocation based on QoS policy. This command is executed in privileged mode.
<code>show ip rsvp reservation</code>	Displays RSVP reservations for active calls. This command is executed in user mode.
<code>show ip rsvp installed [detail]</code>	Displays RSVP reservation details for active calls. This command is executed in user mode.
<code>bandwidth total default bandwidth</code>	Sets total amount of bandwidth for H.323 traffic allowed in the zone. This command is executed in gatekeeper mode.
<code>show gatekeeper status</code>	Displays the current status of gatekeeper parameters, including maximum and current bandwidth information. This command is executed in user mode.
<code>fair-queue</code>	Enables WFQ on an interface. This command is executed in interface configuration mode.

Job Aids

There are no job aids for this lab activity.

Task 1: Enabling Dial-Peer CAC

In this task, you will configure CAC using dial-peer configuration. You will work within your pod to test concurrent call capabilities using CAC.

Activity Procedure

Complete these steps:

- Step 1** Ensure that you have only one dial peer that points to both telephones of your partner. If necessary, edit your configuration to match the requirement. Use wild card characters in your destination pattern to accomplish this step.
- Step 2** Work with your partner to verify that you can make two concurrent calls between your telephones and the telephones of your partner. Do not go on to the next step until this is confirmed.
- Step 3** Use the **max-conn** command to allow a maximum of one call between your local telephones and the telephones of your partner. This command should be configured in the dial peer that points to the partner telephone numbers.
- Step 4** Working with your partner, have one partner place a call to the other partner. Answer the telephone and leave it off hook.
- Step 5** Enable the **debug voice ccapi individual 6** command and have one partner place a second call between partners.
- Is the call successful? _____
- What does the debug output state? _____
- Step 6** Still working with your partner, leave the first call off hook, hang up the second call, and place a new second call in the reverse direction.
- Is the call successful? _____
- You should be able to assess that dial-peer CAC applies to both inbound and outbound calls collectively, allowing only the configured number of calls in either direction.
- Step 7** Change the value of **max-conn** to allow for two concurrent calls to be placed between partners. Make sure that both partners have reconfigured the value before testing.
- Step 8** Place two concurrent calls between yourself and your partner.
- Are the calls successful? _____
- Step 9** After testing is complete, remove the **max-conn** command from the dial peer to allow for unlimited connections.

Activity Verification

You have completed this task when you attain this result:

- You have the ability to control the number of concurrent calls using dial-peer configuration.

Task 2: CAC with RSVP

In this task, you will configure CAC using RSVP configuration. You will work within your pod to test concurrent call capabilities using CAC.

Activity Procedure

Complete these steps:

- Step 1** You will use your PPP serial connection for call routing in this lab. Shut down your Frame Relay serial interface and enable your PPP serial interface.
- Step 2** Enable WFQ on your PPP serial interface and configure the bandwidth for 72 kbps.
- Step 3** Edit your VoIP dial peer pointing toward the telephones of your partner to use the partner PPP serial interface IP address for the session target definition.
- Step 4** Work with your partner to verify that you can make two concurrent calls between your telephones and the partner telephones. Do not go on to the next step until this is confirmed.
- Step 5** Enable RSVP on your PPP interface and set the bandwidth to 10 kbps. Because RTP header compression is enabled on the interface and G.729 codec is used across the WAN interface, 10 kbps will be sufficient bandwidth to carry each call.
- Step 6** Configure the dial peer pointing to the partner telephones to use RSVP by setting both the **req-qos** and **acc-qos** to be **guaranteed-delay**.

Note Do not begin testing until both you and your partner have completed Step 1 through Step 6.

- Step 7** Enable RSVP debugging to view QoS resource reservation as test calls are being made.
- Step 8** Working with your partner, have *only* one partner place a call to the other partner. Answer the telephone and leave it off hook. Use the various RSVP **show** commands to view current reservation information.
 - How many reservations do you see? _____
 - How can you explain the number of reservations? _____
 - How much bandwidth has been allocated for each reservation? _____
 - How much bandwidth would have been allocated if RTP header compression was not turned on? _____
- Step 9** Place a second call between partners. Did the call succeed? _____
 - What did the debug report? _____
 - How much bandwidth will you need to support two calls if RTP header compression is turned on? _____

Step 10 Configure the RSVP bandwidth to support two calls. Place two concurrent calls between partners. It does not matter in which direction the calls flow.

Were both calls successful? _____

How many reservations does the **show** command report? _____

Activity Verification

You have completed this task when you attain this result:

- You have the ability to control the number of concurrent calls using RSVP configuration.

Task 3: CAC with Gatekeeper

In this task, you will configure CAC using gatekeeper configuration. You will work within your pod to test concurrent call capabilities using CAC.

Activity Procedure

Complete these steps:

- Step 1** To properly demonstrate gatekeeper CAC, you will need to remove the RSVP configuration created in the Task 2. Edit your dial peer pointing to the telephones of your partner to remove the **req-qos** and **acc-qos** configuration. Edit your PPP serial interface to remove the **ip rsvp bandwidth** configuration.
- Step 2** Edit your VoIP dial peer pointing toward the partner telephones to use your gatekeeper for call processing using the **session target ras** command.
- Step 3** Because you will be testing only within your own pod, add the gatekeeper of your partner to your gatekeeper configuration using the **zone remote** and **zone prefix** commands.
- Step 4** Work with your partner to verify that you can make two concurrent calls between your telephones and the partner telephones. While the concurrent calls are off hook, use the **show gatekeeper status** command to determine the maximum remote bandwidth allowed and the current remote bandwidth used.

What is the maximum bandwidth? _____

What is the current bandwidth? _____

Note Do not go on to the next step until this step is completed successfully by both partners.

Step 5 Configure your gatekeeper to allow a maximum of 20 kbps bandwidth in total for the zone using the **bandwidth total default** command.

Step 6 Attempt to make two concurrent calls. Are they both successful? _____

Step 7 While a call is off hook, use the **show** command to confirm your maximum and current bandwidth usage.

What is the maximum bandwidth? _____

What is the current bandwidth? _____

Note Do not go on to the next step until this step is completed successfully by both partners.

Step 8 Edit the gatekeeper bandwidth setting to allow two concurrent calls. This setting must match on both routers within the pod before additional calls will be allowed.

What bandwidth setting is required to support two calls? _____

Step 9 Place two concurrent calls between partners. It does not matter in which direction the calls flow.

Were both calls successful? _____

Activity Verification

You have completed this task when you attain this result:

- You have the ability to control the number of concurrent calls using gatekeeper configuration.

Answer Key

The correct answers and expected solutions for the activities that are described in this guide appear here.

Note Sample router configurations shown in the answer key may differ from actual configuration output based on IOS version and hardware platforms used.

Lab 2-1 Answer Key: Connecting a Voice-Enabled Router

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Pod3R1
!
enable password san-fran
!
ip subnet-zero
!
!
ip host Pod3R2 192.168.1.32
ip host Pod3R1 192.168.1.31
ip host Pod2R2 192.168.1.22
ip host Pod2R1 192.168.1.21
ip host Pod1R2 192.168.1.12
ip host Pod1R1 192.168.1.11
!
voice call carrier capacity active
!
mta receive maximum-recipients 0
!
interface Ethernet0/0
 ip address 10.3.10.1 255.255.255.0
 half-duplex
!
interface Serial0/0
```

```

ip address 192.168.1.31 255.255.255.0
encapsulation frame-relay
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Serial0/1
description PPP to Pod3R1
ip address 10.3.3.1 255.255.255.0
encapsulation ppp
!
router eigrp 100
network 10.0.0.0
network 192.168.1.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip http server
!
call rsvp-sync
!
voice-port 2/1/0
!
voice-port 2/1/1
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
shutdown
!
!
line con 0
line aux 0
line vty 0 4
password router
login

```

```
!  
!  
end
```

Lab 2-2 Answer Key: Configuring Voice Interfaces

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!  
version 12.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Pod1R1  
!  
enable password san-fran  
!  
voice-card 1  
!  
ip subnet-zero  
!  
!  
!  
!  
voice call carrier capacity active  
!  
!  
!  
!  
!  
!  
!  
!  
!  
mta receive maximum-recipients 0  
!  
controller T1 1/0  
    framing esf  
    clock source internal
```

```

linecode b8zs
ds0-group 1 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
 framing sf
 linecode ami
!
!
!
!
interface Ethernet0/0
 ip address 10.1.10.1 255.255.255.0
 half-duplex
!
interface Serial0/0
 ip address 192.168.1.11 255.255.255.0
 encapsulation frame-relay
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
interface Serial0/1
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 100
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless

```

```
ip http server
!
!
!
route-map eirgp permit 100
!
!
call rsvp-sync
!
voice-port 1/0:1
  output attenuation 0
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
  cptone AU
  ring cadence define 4 1 8 10
!
voice-port 2/1/1
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
gatekeeper
  shutdown
!
!
line con 0
  password router
  logging synchronous
  login
line aux 0
line vty 0 4
```

```
password router
login
line vty 5 15
password router
login
!
!
end
```

Lab 2-3 Answer Key: Configuring POTS Dial Peers

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Pod1R1
!
enable password 7 08324D40441F17161C
!
voice-card 1
!
ip subnet-zero
!
!
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
```

```

!
mta receive maximum-recipients 0
!
controller T1 1/0
    framing esf
    clock source internal
    linecode b8zs
    ds0-group 1 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
    framing sf
    linecode ami
!
!
!
!
interface Ethernet0/0
    ip address 10.1.10.1 255.255.255.0
    half-duplex
!
interface Serial0/0
    ip address 192.168.1.11 255.255.255.0
    encapsulation frame-relay
!
interface Ethernet0/1
    no ip address
    shutdown
    half-duplex
!
interface Serial0/1
    ip address 10.1.1.1 255.255.255.0
    encapsulation ppp
!
interface FastEthernet3/0
    no ip address
    shutdown
    duplex auto
    speed auto
!
router eigrp 100

```



```

network 10.0.0.0
network 192.168.1.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip http server
!
!
!
route-map eigrp permit 100
!
!
call rsvp-sync
!
voice-port 1/0:1
  output attenuation 0
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
  cptone AU
  ring cadence define 4 1 8 10
!
voice-port 2/1/1
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 1101 pots
  destination-pattern 1101
  port 2/1/0
!
dial-peer voice 1102 pots

```

```

destination-pattern 1102
port 2/1/1
!
dial-peer voice 3 pots
destination-pattern 555....
port 2/0/0
forward-digits all
!
dial-peer voice 4 pots
preference 1
destination-pattern 1109
port 2/1/0
!
dial-peer voice 5 pots
preference 2
destination-pattern 1109
port 2/1/1
!
dial-peer voice 6 pots
destination-pattern 1151
port 1/0:1
forward-digits all
!
dial-peer hunt 7
!
gatekeeper
shutdown
!
!
line con 0
password 7 131718071F0916
logging synchronous
login
line aux 0
line vty 0 4
password 7 111B1610031719
login
line vty 5 15
password 7 02140B4E1F031D
login

```

```
!  
!  
end
```

Lab 2-4 Answer Key: Configuring Special-Purpose Connections

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!  
version 12.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Pod1R1  
!  
enable password 7 08324D40441F17161C  
!  
voice-card 1  
!  
ip subnet-zero  
!  
!  
!  
!  
voice call carrier capacity active  
!  
!  
!  
!  
!  
!  
!  
!  
mta receive maximum-recipients 0  
!  
controller T1 1/0
```

```

framing esf
clock source internal
linecode b8zs
ds0-group 1 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
framing sf
linecode ami
!
!
!
!
interface Ethernet0/0
ip address 10.1.10.1 255.255.255.0
half-duplex
!
interface Serial0/0
ip address 192.168.1.11 255.255.255.0
encapsulation frame-relay
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Serial0/1
ip address 10.1.1.1 255.255.255.0
encapsulation ppp
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 100
network 10.0.0.0
network 192.168.1.0
no auto-summary
no eigrp log-neighbor-changes

```

```

!
ip classless
ip http server
!
!
!
route-map eirgp permit 100
!
!
call rsvp-sync
!
voice-port 1/0:1
  output attenuation 0
  connection Tie-line 7
!
voice-port 2/0/0
  connection plar opx 1102
!
voice-port 2/0/1
!
voice-port 2/1/0
  cptone AU
  ring cadence define 4 1 8 10
!
voice-port 2/1/1
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 1101 pots
  destination-pattern 1101
  port 2/1/0
!
dial-peer voice 1102 pots
  destination-pattern 1102
  port 2/1/1

```

```

!
dial-peer voice 3 pots
  destination-pattern 555....
  port 2/0/0
  forward-digits all
!
dial-peer voice 4 pots
  preference 1
  destination-pattern 1109
  port 2/1/0
!
dial-peer voice 5 pots
  preference 2
  destination-pattern 1109
  port 2/1/1
!
dial-peer voice 6 pots
  destination-pattern 1151
  port 1/0:1
  forward-digits all
!
dial-peer voice 7 voip
  destination-pattern 7....
  session target ipv4:10.1.1.2
!
dial-peer voice 8 pots
  destination-pattern 8....
  port 1/0:1
!
dial-peer hunt 7
!
gatekeeper
  shutdown
!
!
line con 0
  exec-timeout 0 0
  password 7 131718071F0916
  logging synchronous
  login

```

```
line aux 0
line vty 0 4
  password 7 111B1610031719
  login
line vty 5 15
  password 7 02140B4E1F031D
  login
!
!
end
```

Lab 2-5 Answer Key: Configuring Basic VoIP Network Connections

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Pod3R1
!
enable password san-fran
!
memory-size iomem 10
voice-card 1
!
ip subnet-zero
!
!
ip host Pod1R1 192.168.1.11
ip host Pod1R2 192.168.1.12
ip host Pod2R1 192.168.1.21
ip host Pod2R2 192.168.1.22
ip host Pod3R1 192.168.1.31
ip host Pod3R2 192.168.1.32
!
!
```

```

!
voice call carrier capacity active
!
voice class codec 1
  codec preference 1 g711ulaw
  codec preference 2 g729r8
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
controller T1 1/0
  framing esf
  clock source internal
  linecode b8zs
  ds0-group 1 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
  framing sf
  linecode ami
!
!
!
!
interface Ethernet0/0
  ip address 10.3.10.1 255.255.255.0
  half-duplex
!
interface Serial0/0
  ip address 192.168.1.31 255.255.255.0
  encapsulation frame-relay
  frame-relay ip rtp header-compression
!
interface Ethernet0/1

```



```
no ip address
shutdown
half-duplex
!
interface Serial0/1
description PPP to Pod3R1
ip address 10.3.3.1 255.255.255.0
encapsulation ppp
ip tcp header-compression iphc-format
ip rtp header-compression iphc-format
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 100
network 10.0.0.0
network 192.168.1.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip http server
!
!
!
!
call rsvp-sync
!
voice-port 1/0:1
output attenuation 0
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
ring cadence pattern05
```

```

!
voice-port 2/1/1
    ring cadence pattern05
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
    destination-pattern 3101
    port 2/1/0
!
dial-peer voice 2 pots
    destination-pattern 3102
    port 2/1/1
!
dial-peer voice 3 pots
    destination-pattern 9.....
    port 2/0/0
!
dial-peer voice 91 pots
    preference 2
    destination-pattern 3109
    port 2/1/0
!
dial-peer voice 92 pots
    preference 1
    destination-pattern 3109
    port 2/1/1
!
dial-peer voice 20 pots
    destination-pattern 3151
    port 1/0:1
    forward-digits all
!
dial-peer voice 11 voip
    destination-pattern 3201

```

```

voice-class codec 1
session target ipv4:10.3.3.2
!
dial-peer voice 12 voip
destination-pattern 3202
voice-class codec 1
session target ipv4:192.168.1.32
!
dial-peer voice 319 voip
destination-pattern 21..
session target ipv4:192.168.1.21
!
dial-peer hunt 7
!
gatekeeper
shutdown
!
!
line con 0
line aux 0
line vty 0 4
password router
login
!
!
end

```

Lab 3-1 Answer Key: Configuring VoIP with H.323

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```

!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Pod1R1
!
enable password 7 08324D40441F17161C

```

```

!
voice-card 1
!
ip subnet-zero
!
!
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
controller T1 1/0
    framing esf
    clock source internal
    linecode b8zs
    ds0-group 1 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
    framing sf
    linecode ami
!
!
!
!
interface Loopback1
    no ip address
!
interface Ethernet0/0
    ip address 10.1.10.1 255.255.255.0
    half-duplex

```

```

h323-gateway voip interface
h323-gateway voip id gkp1r1 ipaddr 10.1.10.1 1719
h323-gateway voip h323-id gwP1R1
!
interface Serial0/0
 ip address 192.168.1.11 255.255.255.0
 encapsulation frame-relay
 frame-relay ip rtp header-compression
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
interface Serial0/1
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 ip tcp header-compression iphc-format
 ip rtp header-compression iphc-format
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 100
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip classless
ip http server
!
!
!
route-map eigrp permit 100
!
!

```

```

call rsvp-sync
!
voice-port 1/0:1
  output attenuation 0
  connection Tie-line 7
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
!
voice-port 2/1/1
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 1101 pots
  destination-pattern 1101
  port 2/1/0
!
dial-peer voice 1102 pots
  destination-pattern 1102
  port 2/1/1
!
dial-peer voice 3 pots
  destination-pattern 555....
  port 2/0/0
  forward-digits all
!
dial-peer voice 4 pots
  preference 1
  destination-pattern 1109
  port 2/1/0
!
dial-peer voice 5 pots

```

```

preference 2
destination-pattern 1109
port 2/1/1
!
dial-peer voice 6 pots
destination-pattern 1151
port 1/0:1
forward-digits all
!
dial-peer voice 7 voip
destination-pattern 7....
session target ipv4:10.1.1.2
!
dial-peer voice 8 pots
destination-pattern 8....
port 1/0:1
!
dial-peer voice 9 voip
destination-pattern 1201
session target ipv4:10.1.1.2
!
dial-peer voice 10 voip
destination-pattern 1202
session target ipv4:10.1.1.2
!
dial-peer voice 11 voip
destination-pattern ....
session target ras
!
dial-peer hunt 7
gateway
!
!
gatekeeper
zone local gkp1r1 cisco.com 10.1.10.1
zone remote gkp2r1 cisco.com 10.2.10.1 1719
zone remote gkp2r2 cisco.com 10.2.20.1 1719
zone remote gkp3r1 cisco.com 10.3.10.1 1719
zone remote gkp3r2 cisco.com 10.3.20.1 1719
zone prefix gkp2r1 21..

```

```

zone prefix gkp2r2 22..
zone prefix gkp3r1 31..
zone prefix gkp3r2 32..
no shutdown
!
!
line con 0
  exec-timeout 0 0
  password 7 131718071F0916
  logging synchronous
  login
line aux 0
line vty 0 4
  password 7 111B1610031719
  login
line vty 5 15
  password 7 02140B4E1F031D
  login
!
!
end

```

Lab 3-2 Answer Key: Configuring VoIP with SIP

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```

!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Pod1R1
!
enable password 7 08324D40441F17161C
!
voice-card 1
!
ip subnet-zero
!

```



```

!
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
controller T1 1/0
    framing esf
    clock source internal
    linecode b8zs
    ds0-group 1 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
    framing sf
    linecode ami
!
!
!
!
interface Loopback1
    no ip address
!
interface Ethernet0/0
    ip address 10.1.10.1 255.255.255.0
    half-duplex
    h323-gateway voip interface
    h323-gateway voip id gkp1r1 ipaddr 10.1.10.1 1719
    h323-gateway voip h323-id gwP1R1
!
interface Serial0/0

```

```

ip address 192.168.1.11 255.255.255.0
encapsulation frame-relay
frame-relay ip rtp header-compression
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Serial0/1
ip address 10.1.1.1 255.255.255.0
encapsulation ppp
ip tcp header-compression iphc-format
ip rtp header-compression iphc-format
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 100
network 10.0.0.0
network 192.168.1.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip http server
!
!
!
route-map eigrp permit 100
!
!
call rsvp-sync
!
voice-port 1/0:1
output attenuation 0
connection Tie-line 7

```

```

!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
!
voice-port 2/1/1
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 1101 pots
  destination-pattern 1101
  port 2/1/0
!
dial-peer voice 1102 pots
  destination-pattern 1102
  port 2/1/1
!
dial-peer voice 3 pots
  destination-pattern 555....
  port 2/0/0
  forward-digits all
!
dial-peer voice 4 pots
  preference 1
  destination-pattern 1109
  port 2/1/0
!
dial-peer voice 5 pots
  preference 2
  destination-pattern 1109
  port 2/1/1
!
dial-peer voice 6 pots

```

```

destination-pattern 1151
port 1/0:1
forward-digits all
!
dial-peer voice 7 voip
destination-pattern 7....
session target ipv4:10.1.1.2
!
dial-peer voice 8 pots
destination-pattern 8....
port 1/0:1
!
dial-peer voice 9 voip
destination-pattern 1201
session protocol sipv2
session target ipv4:10.1.1.2
!
dial-peer voice 10 voip
destination-pattern 1202
session protocol sipv2
session target ipv4:10.1.1.2
!
dial-peer voice 11 voip
destination-pattern ....
session target ras
!
dial-peer hunt 7
gateway
!
sip-ua
no oli
!
!
gatekeeper
zone local gkp1r1 cisco.com 10.1.10.1
zone remote gkp2r1 cisco.com 10.2.10.1 1719
zone remote gkp2r2 cisco.com 10.2.20.1 1719
zone remote gkp3r1 cisco.com 10.3.10.1 1719
zone remote gkp3r2 cisco.com 10.3.20.1 1719
zone prefix gkp2r1 21..

```

```

zone prefix gkp2r2 22..
zone prefix gkp3r1 31..
zone prefix gkp3r2 32..
no shutdown
!
!
line con 0
exec-timeout 0 0
password 7 131718071F0916
logging synchronous
login
line aux 0
line vty 0 4
password 7 111B1610031719
login
line vty 5 15
password 7 02140B4E1F031D
login
!
!
end

```

Lab 3-3 Answer Key: Configuring VoIP with MGCP

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```

!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Pod1R1
!
enable password 7 08324D40441F17161C
!
voice-card 1
!
ip subnet-zero
!

```

```

!
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
controller T1 1/0
    framing esf
    clock source internal
    linecode b8zs
    ds0-group 1 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
    framing sf
    linecode ami
!
!
!
!
interface Loopback1
    no ip address
!
interface Ethernet0/0
    ip address 10.1.10.1 255.255.255.0
    half-duplex
    h323-gateway voip interface
    h323-gateway voip id gkp1r1 ipaddr 10.1.10.1 1719
    h323-gateway voip h323-id gwP1R1
!
interface Serial0/0

```

```

ip address 192.168.1.11 255.255.255.0
encapsulation frame-relay
frame-relay ip rtp header-compression
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Serial0/1
ip address 10.1.1.1 255.255.255.0
encapsulation ppp
ip tcp header-compression iphc-format
ip rtp header-compression iphc-format
!
interface FastEthernet3/0
no ip address
shutdown
duplex auto
speed auto
!
router eigrp 100
network 10.0.0.0
network 192.168.1.0
no auto-summary
no eigrp log-neighbor-changes
!
ip classless
ip http server
!
!
!
route-map eigrp permit 100
!
!
call rsvp-sync
!
voice-port 1/0:1
output attenuation 0
connection Tie-line 7

```

```

!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
!
voice-port 2/1/1
!
!
mgcp
mgcp call-agent 192.168.100.100 service-type mgcp version 0.1
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
dial-peer voice 1101 pots
  port 2/0/0
  application mgcpapp
!
dial-peer voice 1102 pots
  port 2/0/1
  application mgcpapp
!
dial-peer voice 3 pots
  destination-pattern 555....
  port 2/0/0
  forward-digits all
!
dial-peer voice 6 pots
  destination-pattern 1151
  port 1/0:1
  forward-digits all
!
dial-peer voice 7 voip
  destination-pattern 7....

```



```

    session target ipv4:10.1.1.2
    !
dial-peer voice 8 pots
    destination-pattern 8....
    port 1/0:1
    !
dial-peer voice 9 voip
    destination-pattern 1201
    session protocol sipv2
    session target ipv4:10.1.1.2
    !
dial-peer voice 10 voip
    destination-pattern 1202
    session protocol sipv2
    session target ipv4:10.1.1.2
    !
dial-peer voice 11 voip
    destination-pattern ....
    session target ras
    !
dial-peer hunt 7
gateway
!
sip-ua
    no oli
!
!
gatekeeper
    zone local gkp1r1 cisco.com 10.1.10.1
    zone remote gkp2r1 cisco.com 10.2.10.1 1719
    zone remote gkp2r2 cisco.com 10.2.20.1 1719
    zone remote gkp3r1 cisco.com 10.3.10.1 1719
    zone remote gkp3r2 cisco.com 10.3.20.1 1719
    zone prefix gkp2r1 21..
    zone prefix gkp2r2 22..
    zone prefix gkp3r1 31..
    zone prefix gkp3r2 32..
    no shutdown
!
!

```

```

line con 0
  exec-timeout 0 0
  password 7 131718071F0916
  logging synchronous
  login
line aux 0
line vty 0 4
  password 7 111B1610031719
  login
line vty 5 15
  password 7 02140B4E1F031D
  login
!
!
end

```

Lab 4-1 Answer Key: Implementing Cisco AutoQoS

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Pod1R1
!
boot-start-marker
boot-end-marker
!
enable password 7 08324D40441F17161C
!
voice-card 1
!
no aaa new-model
ip subnet-zero
!
!
!
!
!

```

```
ip cef
!
!
voice call carrier capacity active
!
!
!
!
!
!
!
!
!
!
!

controller T1 1/0
    framing esf
    crc-threshold 320
    clock source internal
    linecode b8zs
    ds0-group 1 timeslots 1-12 type e&m-wink-start
!
class-map match-any AutoQoS-VoIP-Remark
    match ip dscp ef
    match ip dscp cs3
    match ip dscp af31
class-map match-any AutoQoS-VoIP-Control-UnTrust
    match access-group name AutoQoS-VoIP-Control
class-map match-any AutoQoS-VoIP-RTP-UnTrust
    match protocol rtp audio
    match access-group name AutoQoS-VoIP-RTCP
!
!
policy-map AutoQoS-Policy-UnTrust
    class AutoQoS-VoIP-RTP-UnTrust
        priority percent 70
        set dscp ef
    class AutoQoS-VoIP-Control-UnTrust
```

```

    bandwidth percent 5
    set dscp af31
class AutoQoS-VoIP-Remark
    set dscp default
class class-default
    fair-queue
!
!
!
!
interface Loopback1
    no ip address
!
interface Ethernet0/0
    ip address 10.1.10.1 255.255.255.0
    half-duplex
    h323-gateway voip interface
    h323-gateway voip id gkp1r1 ipaddr 10.1.10.1 1719
    h323-gateway voip h323-id gwP1R1
!
interface Serial0/0
    no ip address
    encapsulation frame-relay
    frame-relay traffic-shaping
    frame-relay ip rtp header-compression
!
interface Serial0/0.1 point-to-point
    bandwidth 72
    ip address 192.168.1.11 255.255.255.0
    frame-relay interface-dlci 102
        class AutoQoS-VoIP-FR-Serial0/0-102
            auto qos voip
    frame-relay ip rtp header-compression
!
interface Serial0/1
    no ip address
    encapsulation ppp
    ip tcp header-compression iphc-format
    shutdown
    clockrate 72000

```

```

ip rtp header-compression iphc-format
!
router eigrp 100
network 10.0.0.0
network 192.168.1.0
no auto-summary
no eigrp log-neighbor-changes
!
ip http server
ip classless
!
!
!
ip access-list extended AutoQoS-VoIP-Control
permit tcp any any eq 1720
permit tcp any any range 11000 11999
permit udp any any eq 2427
permit tcp any any eq 2428
permit tcp any any range 2000 2002
permit udp any any eq 1719
permit udp any any eq 5060
ip access-list extended AutoQoS-VoIP-RTCP
permit udp any any range 16384 32767
!
map-class frame-relay AutoQoS-VoIP-FR-Serial0/0-102
frame-relay cir 72000
frame-relay bc 720
frame-relay be 0
frame-relay mincir 72000
service-policy output AutoQoS-Policy-UnTrust
frame-relay fragment 90
!
route-map eigrp permit 100
!
!
!
control-plane
!
rmon event 33333 log trap AutoQoS description "AutoQoS SNMP
traps for Voice Drop
s" owner AutoQoS

```

```

rmon alarm 33333 cbQosCMDropBitRate.1081.1083 30 absolute
rising-threshold 1 333
33 falling-threshold 0 owner AutoQoS
!
!
voice-port 1/0:1
  output attenuation 0
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
!
voice-port 2/1/1
!
!
!
!
dial-peer cor custom
!
!
!
dial-peer voice 1101 pots
  destination-pattern 1101
  port 2/1/0
!
dial-peer voice 1102 pots
  destination-pattern 1102
  port 2/1/1
!
dial-peer voice 3 pots
  destination-pattern 555....
  port 2/0/0
  forward-digits all
!
dial-peer voice 6 pots
  destination-pattern 1151
  port 1/0:1
  forward-digits all
!

```

```

dial-peer voice 7 voip
  destination-pattern 7....
  session target ipv4:10.1.1.2
!
dial-peer voice 8 pots
  destination-pattern 8....
  port 1/0:1
!
dial-peer voice 9 voip
  destination-pattern 1201
  session target ipv4:192.168.1.12
!
dial-peer voice 10 voip
  destination-pattern 1202
  session target ipv4:192.168.1.12
!
dial-peer voice 11 voip
  destination-pattern ....
  session target ras
!
dial-peer hunt 7
gateway
!
!
gatekeeper
  zone local gkp1r1 cisco.com 10.1.10.1
  zone remote gkp2r1 cisco.com 10.2.10.1 1719
  zone remote gkp2r2 cisco.com 10.2.20.1 1719
  zone remote gkp3r1 cisco.com 10.3.10.1 1719
  zone remote gkp3r2 cisco.com 10.3.20.1 1719
  zone prefix gkp2r1 21..
  zone prefix gkp2r2 22..
  zone prefix gkp3r1 31..
  zone prefix gkp3r2 32..
  no shutdown
!
!
line con 0
  exec-timeout 0 0
  password cisco

```

```

logging synchronous
login
line aux 0
line vty 0 4
password 7 111B1610031719
login
length 0
line vty 5 15
password 7 02140B4E1F031D
login
!
!
!
end

```

Lab 4-2 Answer Key: Implementing CAC (Tasks 1 and 2)

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P2R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$EnK7$IxzFBbU/7Rnr9aENeWHWc/
!
no aaa new-model
!
resource policy
!
memory-size iomem 25
voice-card 1
!
ip subnet-zero
!

```



```

ip cef
no ip domain lookup
!
controller T1 1/0
  framing esf
  clock source internal
  linecode b8zs
  ds0-group 1 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
  framing sf
  linecode ami
!
interface Tunnel1
  no ip address
!
interface Ethernet0/0
  ip address 10.2.10.1 255.255.255.0
  full-duplex
  h323-gateway voip interface
  h323-gateway voip id gkP2R1 ipaddr 10.2.10.1 1719
  h323-gateway voip h323-id gwP2R1
!
interface Serial0/0
  bandwidth 72
  ip address 10.2.2.1 255.255.255.0
  encapsulation ppp
  ip tcp header-compression iphc-format
  clock rate 72000
  fair-queue 64 32 1
  ip rtp header-compression iphc-format
  ip rsvp bandwidth 20
!
interface Ethernet0/1
  no ip address
  shutdown
  half-duplex
!
interface Serial0/1
  ip address 192.168.1.21 255.255.255.0

```

```

encapsulation frame-relay
shutdown
frame-relay ip rtp header-compression
!
router eigrp 100
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
ip http server
ip classless
!
control-plane
!
voice-port 1/0:1
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
 ring cadence define 4 1 8 10
 cptime AU
!
voice-port 2/1/1
!
dial-peer voice 2101 pots
 destination-pattern 2101
 port 2/1/0
!
dial-peer voice 2102 pots
 destination-pattern 2102
 port 2/1/1
!
dial-peer voice 3 pots
 destination-pattern 9555....
 port 2/0/0
 forward-digits 7
!
dial-peer voice 4 pots

```

```

preference 2
destination-pattern 2109
port 2/1/0
!
dial-peer voice 5 pots
preference 1
destination-pattern 2109
port 2/1/1
!
dial-peer voice 6 pots
destination-pattern 2151
port 1/0:1
forward-digits all
!
dial-peer voice 10 voip
destination-pattern 22..
session target ipv4:10.2.2.2
req-qos guaranteed-delay
acc-qos guaranteed-delay
!
dial-peer voice 11 voip
destination-pattern ....
session target ras
!
dial-peer hunt 7
gateway
timer receive-rtp 1200
!
gatekeeper
zone local gkP2R1 cisco.com 10.2.10.1
zone remote gkP1R2 cisco.com 10.1.20.1 1719
zone remote gkP1R1 cisco.com 10.1.10.1 1719
zone remote gkP3R1 cisco.com 10.3.10.1 1719
zone remote gkP3R2 cisco.com 10.3.20.1 1719
zone remote gkP4R1 cisco.com 10.4.10.1 1719
zone remote gkP4R2 cisco.com 10.4.20.1 1719
zone prefix gkP1R1 11..
zone prefix gkP1R2 12..
zone prefix gkP3R1 31..
zone prefix gkP3R2 32..

```

```

zone prefix gkP4R1 41..
zone prefix gkP4R2 42..
bandwidth total default 32
no shutdown
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  password router
  login
!
end

```

Lab 4-2 Answer Key: Implementing CAC (Task 3)

When you complete this activity, your router configuration will be similar to the results here, with differences that are specific to your device or workgroup:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P2R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$EnK7$IxzFBbU/7Rnr9aENeWHWc/
!
no aaa new-model
!
resource policy
!
memory-size iomem 25
voice-card 1
!
ip subnet-zero

```

```

!
!
ip cef
no ip domain lookup
!
!
controller T1 1/0
    framing esf
    clock source internal
    linecode b8zs
    ds0-group 1 timeslots 1-24 type e&m-wink-start
!
controller T1 1/1
    framing sf
    linecode ami
!
!
!
interface Tunnel1
    no ip address
!
interface Ethernet0/0
    ip address 10.2.10.1 255.255.255.0
    full-duplex
    h323-gateway voip interface
    h323-gateway voip id gkP2R1 ipaddr 10.2.10.1 1719
    h323-gateway voip h323-id gwP2R1
!
interface Serial0/0
    bandwidth 72
    ip address 10.2.2.1 255.255.255.0
    encapsulation ppp
    ip tcp header-compression iphc-format
    clock rate 72000
    ip rtp header-compression iphc-format
!
interface Ethernet0/1
    no ip address
    shutdown
    half-duplex

```

```

!
interface Serial0/1
  ip address 192.168.1.21 255.255.255.0
  encapsulation frame-relay
  shutdown
  frame-relay ip rtp header-compression
!
router eigrp 100
  network 10.0.0.0
  network 192.168.1.0
  no auto-summary
!
ip http server
ip classless
!
!
control-plane
!
!
voice-port 1/0:1
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
  ring cadence define 4 1 8 10
  cptone AU
!
voice-port 2/1/1
!
dial-peer voice 2101 pots
  destination-pattern 2101
  port 2/1/0
!
dial-peer voice 2102 pots
  destination-pattern 2102
  port 2/1/1
!
dial-peer voice 3 pots

```

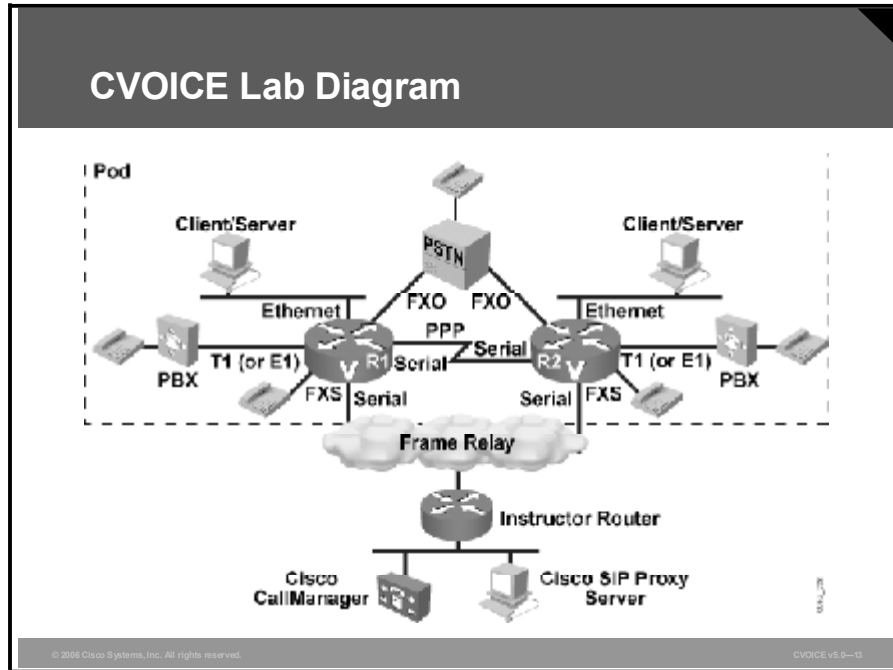
```

destination-pattern 9555....
port 2/0/0
forward-digits 7
!
dial-peer voice 4 pots
preference 2
destination-pattern 2109
port 2/1/0
!
dial-peer voice 5 pots
preference 1
destination-pattern 2109
port 2/1/1
!
dial-peer voice 6 pots
destination-pattern 2151
port 1/0:1
forward-digits all
!
dial-peer voice 10 voip
destination-pattern 22..
session target ras
!
dial-peer voice 11 voip
destination-pattern ....
session target ras
!
dial-peer hunt 7
gateway
timer receive-rtcp 1200
!
!
gatekeeper
zone local gkP2R1 cisco.com 10.2.10.1
zone remote gkP1R2 cisco.com 10.1.20.1 1719
zone remote gkP1R1 cisco.com 10.1.10.1 1719
zone remote gkP3R1 cisco.com 10.3.10.1 1719
zone remote gkP3R2 cisco.com 10.3.20.1 1719
zone remote gkP4R1 cisco.com 10.4.10.1 1719
zone remote gkP4R2 cisco.com 10.4.20.1 1719

```

```
zone remote gkP2R2 cisco.com 10.2.20.1 1719
zone prefix gkP1R1 11..
zone prefix gkP1R2 12..
zone prefix gkP2R2 22..
zone prefix gkP3R1 31..
zone prefix gkP3R2 32..
zone prefix gkP4R1 41..
zone prefix gkP4R2 42..
bandwidth total default 32
no shutdown
!
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  password router
  login
!
!  
end
```


Lab Pull-Out Resource



IP Address Assignment

Pod Number	Device	Client	Ethernet	PPP	Frame Relay
1	R1	10.1.10.100	10.1.10. 1	10.1.1.1	192.168.1.11
	R2	10.1.20.100	10.1.20.1	10.1.1.2	192.168.1.12
2	R1	10.2.10.100	10.2.10.1	10.2.2.1	192.168.1.21
	R2	10.2.20.100	10.2.20.1	10.2.2.2	192.168.1.22
3	R1	10.3.10.100	10.3.10.1	10.3.3.1	192.168.1.31
	R2	10.3.20.100	10.3.20.1	10.3.3.2	192.168.1.32
4	R1	10.4.10.100	10.4.10.1	10.4.4.1	192.168.1.41
	R2	10.4.20.100	10.4.20.1	10.4.4.2	192.168.1.42

Host Name

Pod Number	Router	Host Name
1	R1	Pod1R1
	R2	Pod1R2
2	R1	Pod2R1
	R2	Pod2R2
3	R1	Pod3R1
	R2	Pod3R2
4	R1	Pod4R1
	R2	Pod4R2
5	R1	Pod5R1
	R2	Pod5R2
6	R1	Pod6R1
	R2	Pod6R2

Dial Plan Conventions

As with IP addresses, the dial plan convention allows a student to anticipate the number of any telephone in the classroom. The highlights of the strategy include these points:

- The classroom uses a four-digit dial plan.
- The first digit identifies the pod number (1 to 6).
- The second and third digits identify the device (PSTN=00, R1=10, PBX1=15, R2=20, PBX2=25).
- The fourth digit identifies the telephone.

Classroom Dial Plan

Pod Number		1	2	3	4	5	6
R1		1101	2101	3101	4101	5101	6101
		1102	2102	3102	4102	5102	6102
PBX1		1151	2151	3151	4151	5151	6151
R2		1201	2201	3201	4201	5201	6201
		1202	2202	3202	4202	5202	6202
PBX2		1251	2251	3251	4251	5251	6251
PSTN	Port 1	555-1001	555-2001	555-3001	555-4001	555-5001	555-6001
	Port 2	555-1002	555-2002	555-3002	555-4002	555-5002	555-6002
	Port 3	555-1003	555-2003	555-3003	555-4003	555-5003	555-6003