CVOICE

Cisco Voice over IP

Version 4.1

Student Guide

Text Part Number:

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • 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

LABORATORY EXERCISES

ADDITIONAL RESOURCES

Course Introduction

Overview

The Cisco Voice over IP (CVOICE) course provides an understanding of converged voice and data networks as well as the challenges faced by their various technologies. The course presents Cisco Systems solutions and implementation considerations to address those challenges.

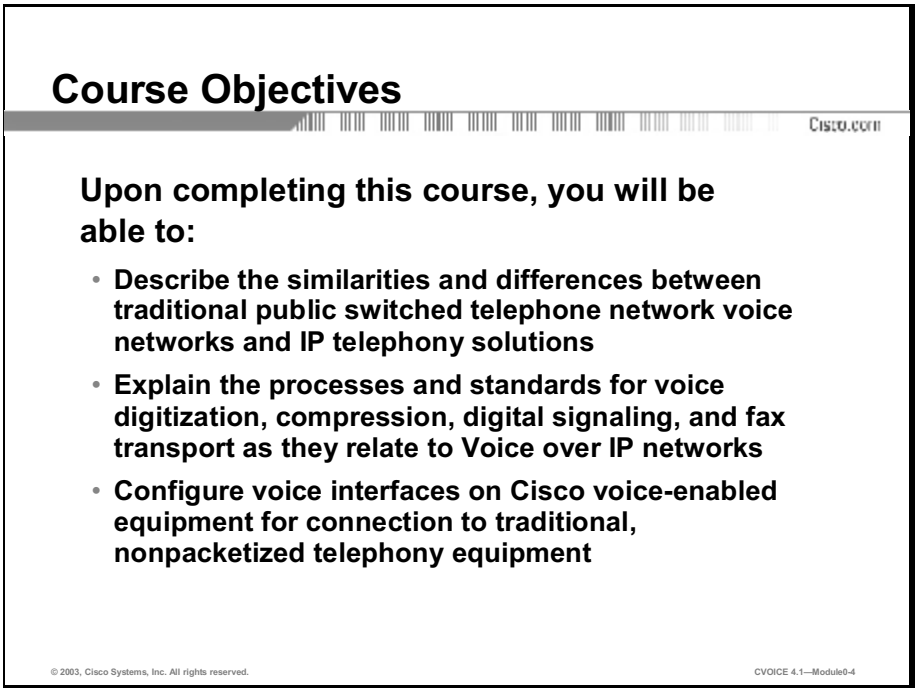
Outline

The Course Introduction includes these topics:

- Course Objectives
- Cisco Certifications
- Learner Skills and Requirements
- Learner Responsibilities
- General Administration
- Course Flow Diagram
- Icons and Symbols
- Learner Introductions
- Course Evaluations

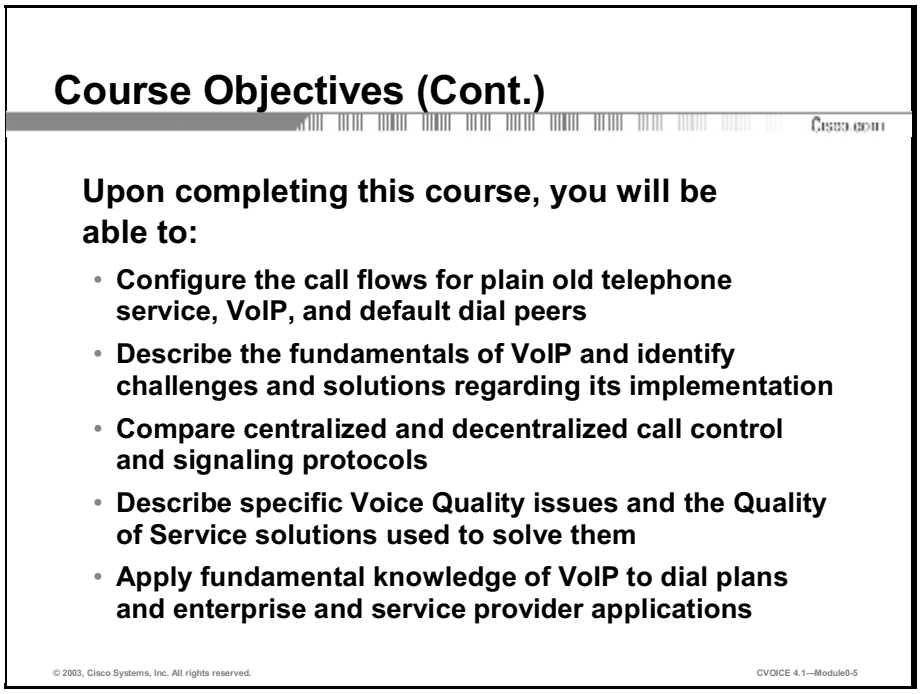
Course Objectives

This topic lists the course objectives.



Upon completing this course, you will be able to:

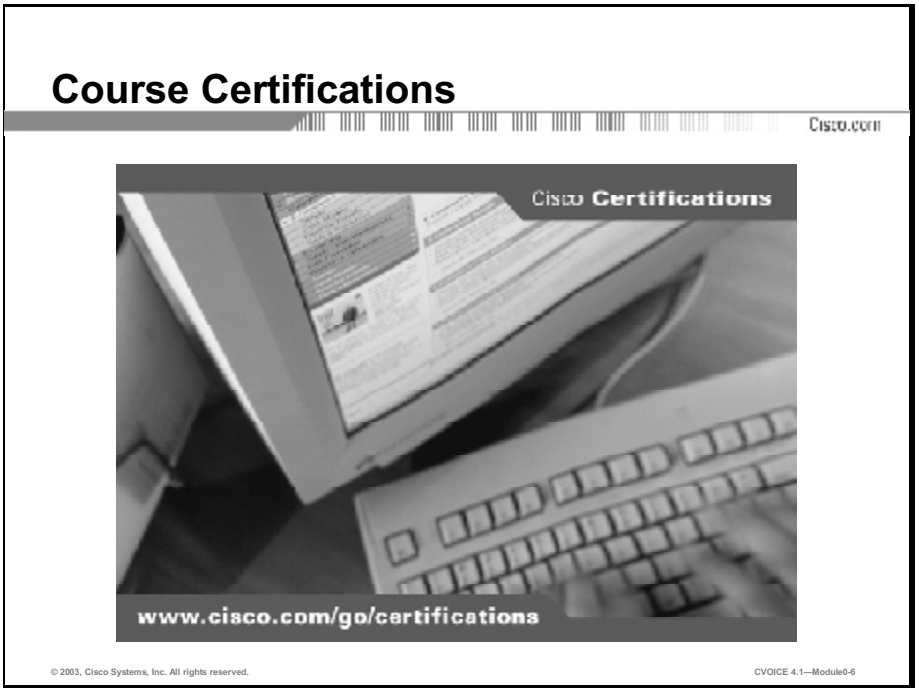
- Describe the similarities and differences between traditional public switched telephone network voice networks and IP telephony solutions
- Explain the processes and standards for voice digitization, compression, digital signaling, and fax transport as they relate to Voice over IP networks
- Configure voice interfaces on Cisco voice-enabled equipment for connection to traditional, nonpacketized telephony equipment



- Configure the call flows for plain old telephone service, VoIP, and default dial peers
- Describe the fundamentals of VoIP and identify challenges and solutions regarding its implementation
- Compare centralized and decentralized call control and signaling protocols
- Describe specific voice quality issues and the quality of service solutions used to solve them
- Apply fundamental knowledge of VoIP to dial plans and enterprise and service provider applications

Cisco Certifications

This topic lists the certification requirements of this course.



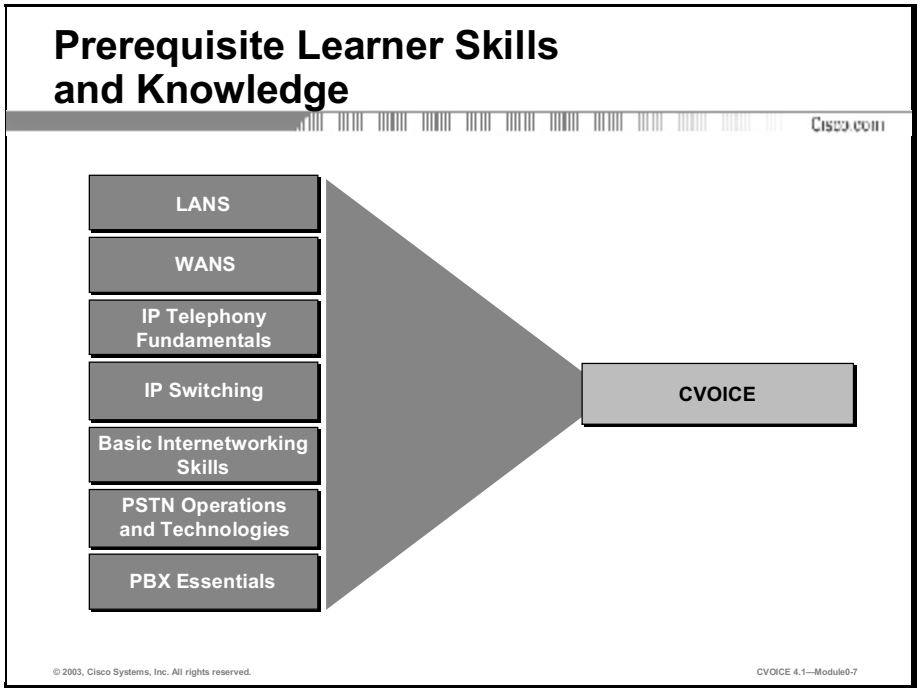
Cisco provides three levels of general career certifications for IT professionals with several different tracks to meet individual needs. Cisco also provides a variety of Cisco Qualified Specialist (CQS) certifications, which enable learners to demonstrate knowledge in specific technologies, solutions, 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.

Reference For additional information on Cisco certification, go to http://www.cisco.com/go/certifications.

Learner Skills and Knowledge

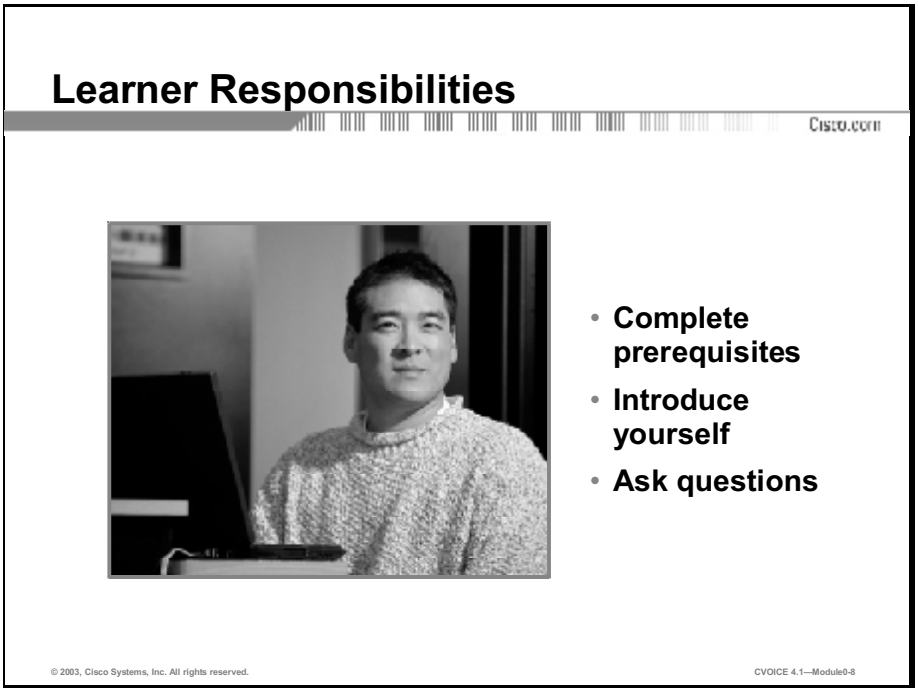
This topic lists the course prerequisites.



By definition, Voice over IP (VoIP) uses an IP internetwork for its voice transport. To fully comprehend the concepts and technologies taught in this course, a working knowledge of LANs, WANs, and IP switching and routing is essential. Basic internetworking skills taught in the "Interconnecting Cisco Network Devices" (ICND) course—or its equivalent—are also necessary. Although this is a packetized voice course, knowledge of traditional public switched telephone network (PSTN) operations and voice fundamentals is required.

Learner Responsibilities

This topic discusses the responsibilities of the learners.



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

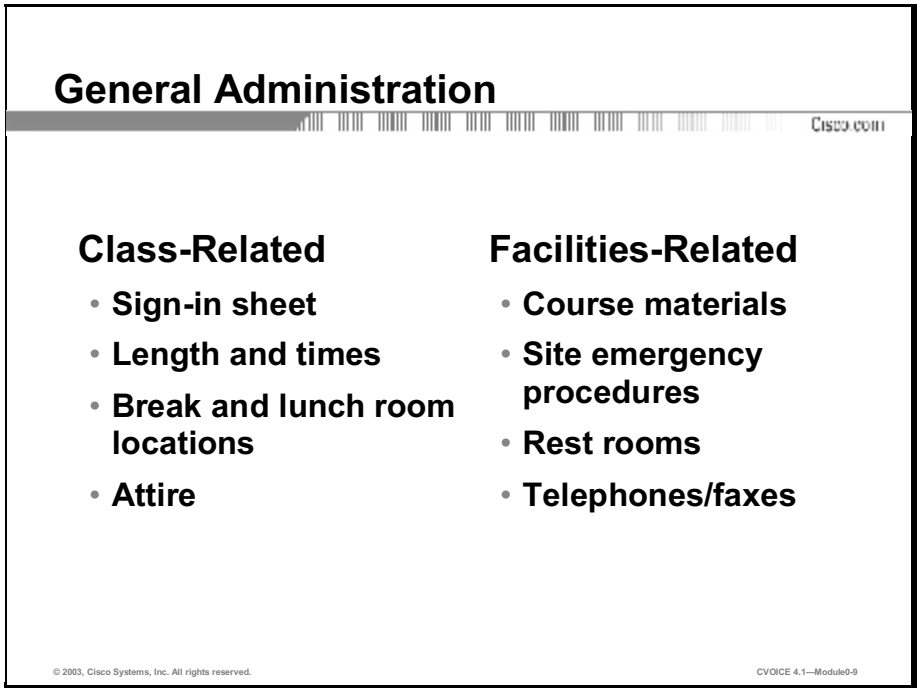
In class, you are expected to participate in all lesson exercises and assessments.

In addition, you are encouraged to ask any questions 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.

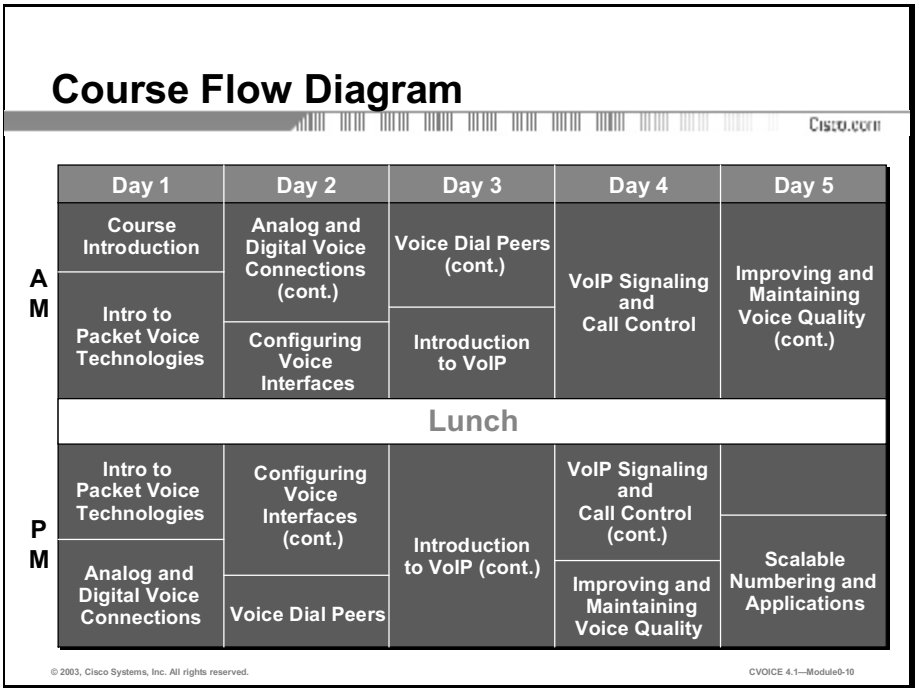


The instructor will discuss the administrative issues noted here so you know exactly what to expect from the class.

- Sign-in process
- Starting and anticipated ending times of each class day
- Class breaks and lunch facilities
- Appropriate attire during class
- Materials 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

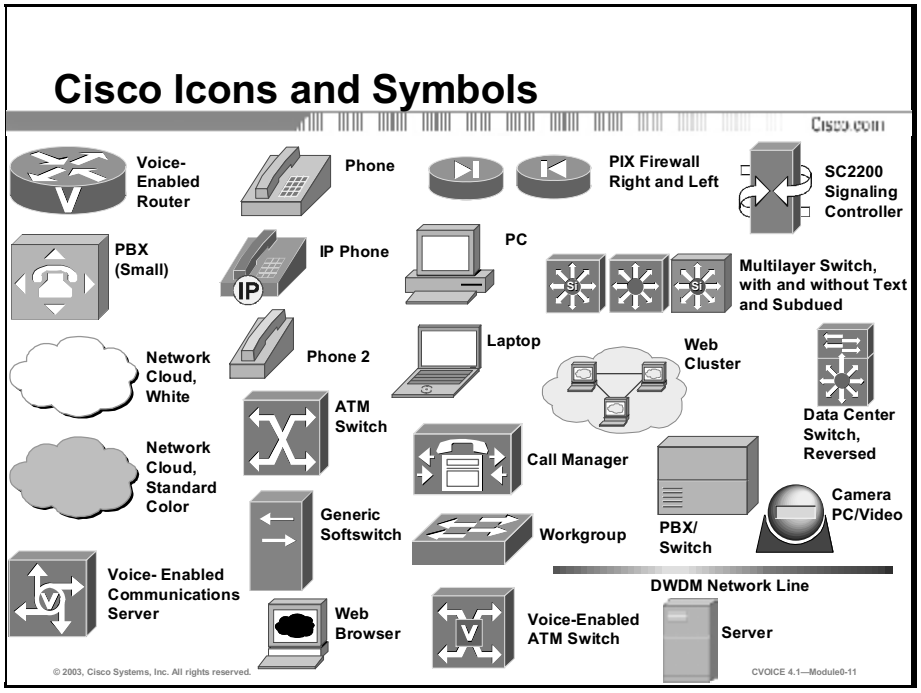
This topic covers the suggested flow of the course materials.



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.

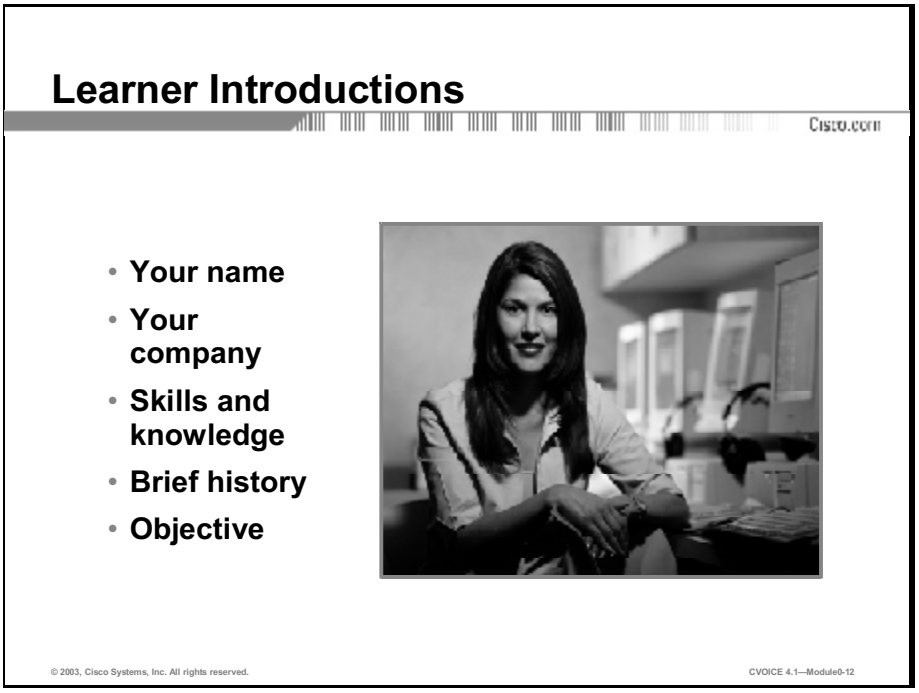
Icons and Symbols

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.



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

Course Evaluations

Cisco relies on customer feedback to make improvements and guide business decisions. Your valuable input will help shape future Cisco learning products and program offerings.

On the first and final days of class, your instructor will provide the following information needed to fill out the evaluation:

- Course acronym *(printed on student kit side label)* _____
- Course version number *(printed on student kit side label)* _____
- Cisco Learning Partner ID # _____
- Instructor ID # _____
- Course ID # *(for courses registered in Cisco Learning Locator)* _____

Please use this information to complete a brief (approximately 10 minutes) online evaluation concerning your instructor and the course materials in the student kit. To access the evaluation, go to http://www.cisco.com/go/clpevals.

After the completed survey has been submitted, you will be able to access links to a variety of Cisco resources, including information on the Cisco Career Certification programs and future Cisco Networkers events.

If you encounter any difficulties accessing the course evaluation URL or submitting your evaluation, please contact Cisco via email at clpevals_support@external.cisco.com.

1

Introduction to Packet Voice Technologies

Overview

Voice over IP (VoIP) is forecasted to have explosive growth in the coming months and years. Many corporate environments have migrated, are actively migrating, or are researching the process of migrating to VoIP. Some long-distance providers are using VoIP to carry voice traffic, particularly on international calls.

Migration is a process that involves gradually phasing out old components and replacing them with new ones. Many terms have been used to describe the technologies and applications for transporting voice in a converged packet network environment. When designing a converged network, it is necessary to clearly define all requirements and understand the various options that are available.

An important first step in designing a converged network is to understand the traditional telephony network and how it interfaces with voice components. You must know, from the start, how legacy voice equipment is connected and their possible migration paths.

The next step towards a good design is being knowledgeable about the components available for Packet Telephony Networks. You should be aware of the difference between voice and data flow within the network and the tools for controlling voice calls. Network requirements vary according to the location size. Knowing the difference between campus, enterprise, and service provider environments is crucial in choosing the right components and technologies.

This module provides an overview of the basic telephony functions and devices, including PBXs, switching functions, call signaling, and multiplexing techniques. It also reviews the basic components of the Packet Telephony Network and identifies the different requirements in campus, enterprise, and service provider environments. Together, these concepts and techniques provide a solid introduction to the VoIP arena.

Upon completing this module, you will be able to:

- Identify the components, processes, and features of traditional telephony networks that provide end-to-end call functionality
- Describe two methods of call control used on voice and data networks and provide one protocol example for each
- List five components or capabilities that are required to provide integrated voice and data services in campus LAN, enterprise, and service provider environments

Outline

The module contains these lessons:

- Traditional Telephony
- Packetized Telephony Networks
- IP Telephony Applications

Traditional Telephony

Overview

This lesson describes the components that make up a traditional telephony network and the process of passing calls through the network.

Importance

In traditional telephony networks, many components and processes are transparent to the customer. As you move from traditional telephony networks to converged voice and data networks, you must manage new components and processes to ensure seamless end-to-end call handling. To maintain acceptable service levels, you must understand which devices must now be supported and the processes that are necessary to ensure end-to-end call functionality.

Objectives

Upon completing this lesson, you will be able to:

- Describe the components and functionality of traditional telephony networks
- Explain how central office switches process telephone calls
- Identify types of private switching systems used in traditional telephony networks and list the main features of each
- Describe the three types of signaling in traditional telephony networks and identify how each is used
- Describe two methods used to multiplex voice in traditional telephony networks

Learner Skills and Knowledge

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

- General knowledge of telephony technology, including customer premises equipment (CPE) and the public switched telephone network (PSTN)

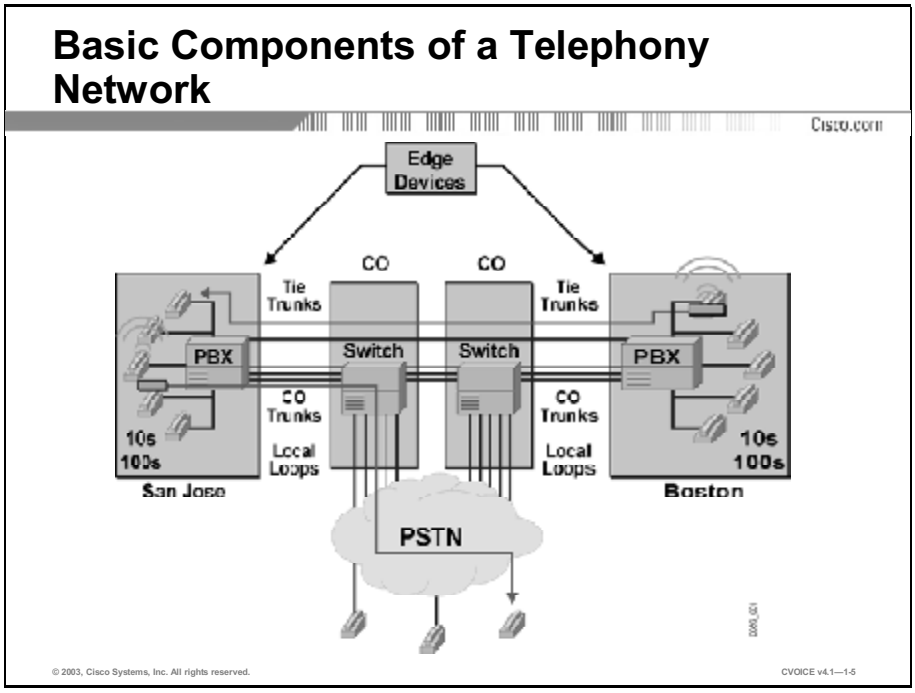
Outline

This lesson includes these topics:

- Overview
- Basic Components of a Telephony Network
- Central Office Switches
- Private Switching Systems
- Call Signaling
- Multiplexing Techniques
- Summary
- Assessment (Quiz): Traditional Telephony

Basic Components of a Telephony Network

This topic introduces the components of traditional telephony networks.



A number of components must be in place for an end-to-end call to succeed. These components are shown in the figure and include the following:

- Edge devices
- Local loops
- Private or central office (CO) switches
- Trunks

Edge Devices

The two types of edge devices that are used in a telephony network include:

- **Analog telephones:** Analog telephones are most common in home, small office/home office (SOHO), and small business environments. Direct connection to the public switched telephone network (PSTN) is usually made by using analog telephones. Proprietary analog telephones are occasionally used in conjunction with a PBX. These phones provide additional functions such as speakerphone, volume control, PBX message-waiting indicator, call on hold, and personalized ringing.

- **Digital telephones:** Digital telephones contain hardware to convert analog voice into a digitized stream. Larger corporate environments with PBXs generally use digital telephones. Digital telephones are typically proprietary, meaning that they work with the PBX or key system of that vendor only.

Local Loops

A local loop is the interface to the telephone company network. Typically, it is a single pair of wires that carry a single conversation. A home or small business may have multiple local loops.

Private or CO Switches

The CO switch terminates the local loop and handles signaling, digit collection, call routing, call setup, and call teardown.

A PBX switch is a privately owned switch located at the customer site. A PBX typically interfaces with other components to provide additional services; for example, voice mail.

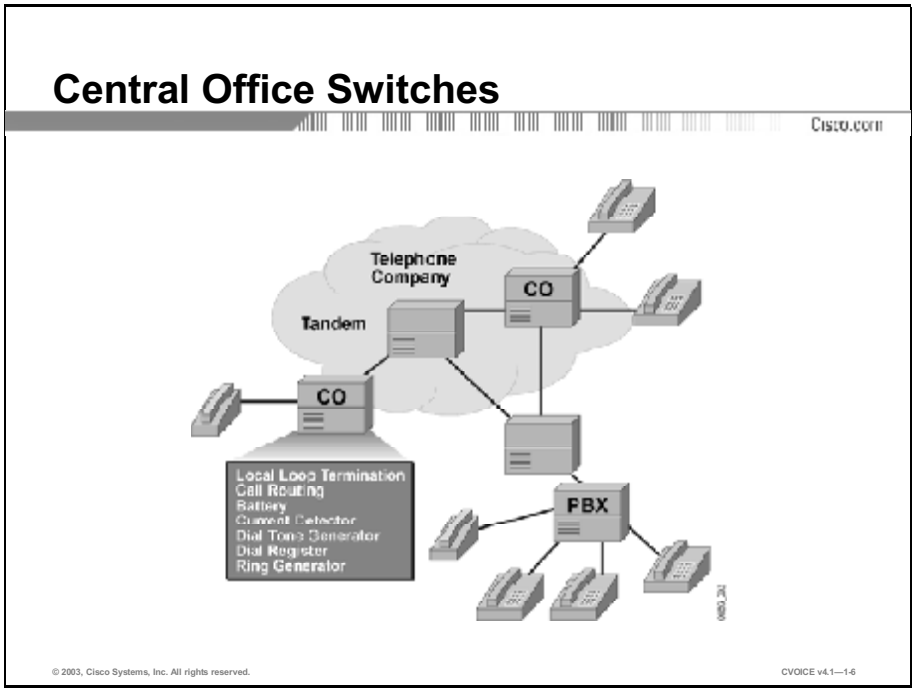
Trunks

The primary function of a trunk is to provide the path between two switches. There are several common trunk types including:

- **Tie trunk:** A dedicated circuit that connects PBXs directly
- **CO trunk:** A direct connection between a local CO and a PBX
- **Interoffice trunk:** A circuit that connects two local telephone company COs.

Central Office Switches

This topic describes how CO switches function and make switching decisions.



The figure shows a typical CO switch environment. The CO switch terminates the local loop and makes the initial call-routing decision.

The call-routing function forwards the call to one of the following:

- Another end-user telephone, if it is connected to the same CO
- Another CO switch
- A tandem switch

The CO switch makes the telephone work with the following components:

- **Battery:** The battery is the source of power to both the circuit and the telephone—it determines the status of the circuit. When the handset is lifted to let current flow, the telephone company provides the source that powers the circuit and the telephone. Because the telephone company powers the telephone from the CO, electrical power outages should not affect the basic telephone.

Note	Some telephones on the market offer additional features that require a supplementary power source that the subscriber supplies; for example, cordless telephones. Some cordless telephones may lose function during a power outage.

- **Current detector:** The current detector monitors the status of a circuit by detecting whether it is open or closed. The table here describes current flow in a typical telephone.

Table 1: Current Flow in a Typical Telephone

Handset	Circuit	Current Flow
On cradle	On hook/open circuit	No
Off cradle	Off hook/closed circuit	Yes

- **Dial tone generator:** When the digit register is ready, the dial-tone generator produces a dial tone to acknowledge the request for service.
- **Digit register:** The digit register receives the dialed digits.
- **Ring generator:** When the switch detects a call for a specific subscriber, the ring generator alerts the called party by sending a ring signal to that subscriber.

You must configure a PBX connection to a CO switch that matches the signaling of the CO switch. This configuration ensures that the switch and the PBX can detect on hook, off hook, and dialed digits coming from either direction.

CO Switching Systems

Switching systems provide three primary functions:

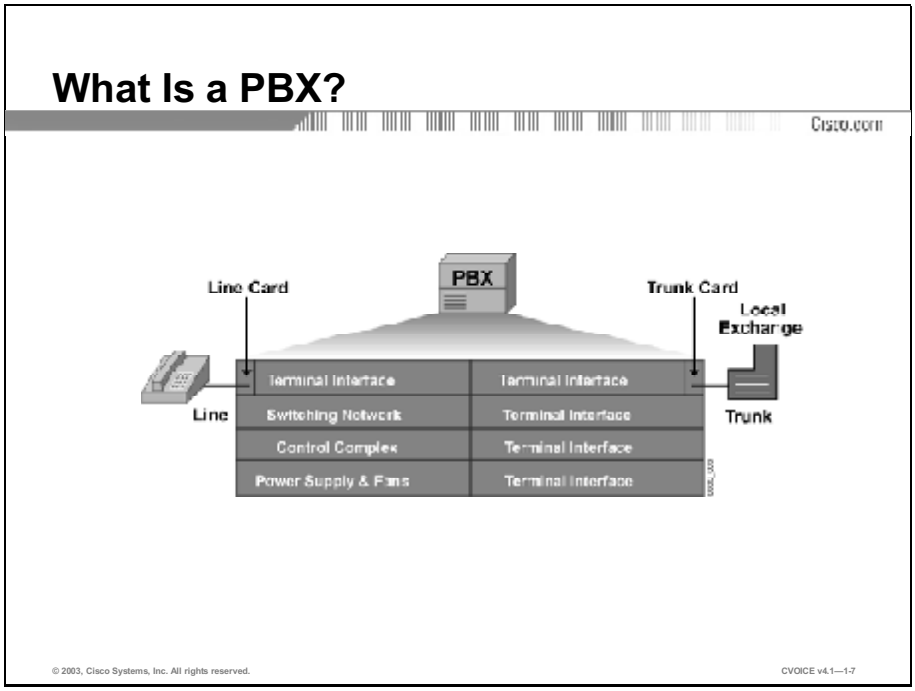
- Call setup, routing, and teardown
- Call supervision
- Customer ID and telephone numbers

CO switches switch calls between locally terminated telephones. If a call recipient is not locally connected, the CO switch decides where to send the call based on its call-routing table. The call then travels over a trunk to another CO or to an intermediate switch that may belong to an inter-exchange carrier (IXC). Although intermediate switches do not provide dial tone, they act as hubs to connect other switches and provide interswitch call routing.

PSTN calls are traditionally circuit-switched, which guarantees end-to-end path and resources. Therefore, as the PSTN sends a call from one switch to another, the same resource is associated with the call until the call is terminated.

Private Switching Systems

In a corporate environment, where large numbers of staff need access to each other and the outside, individual telephone lines are not economically viable. This topic explores PBX and key telephone system functionality in environments today.



A PBX is a smaller, privately owned version of the CO switches used by telephone companies.

Most businesses have a PBX telephone system, a key telephone system, or Centrex service. Large offices with more than 50 telephones or handsets choose a PBX to connect users, both in-house and to the PSTN.

PBXs come in a variety of sizes, typically from 20 to 20,000 stations. The selection of a PBX is important to most companies because a PBX has a typical life span of 7 to 10 years.

All PBXs offer a standard, basic set of calling features. Optional software provides additional capabilities.

The figure illustrates the internal components of a PBX: it connects to telephone handsets using line cards and to the local exchange using trunk cards.

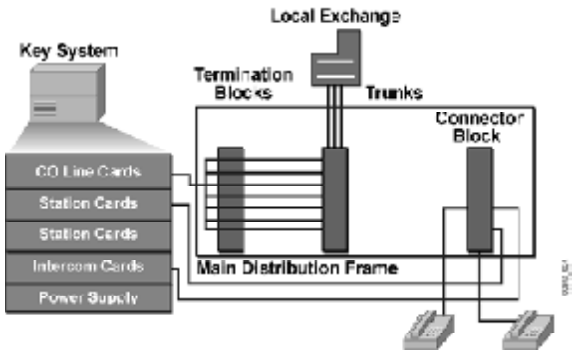
A PBX has three major components:

- **Terminal interface:** The terminal interface provides the connection between terminals and PBX features that reside in the control complex. Terminals can include telephone handsets, trunks, and lines. Common PBX features include dial tone and ringing.

- **Switching network:** The switching network provides the transmission path between two or more terminals in a conversation; for example, two telephones within an office communicate over the switching network.

- **Control complex:** The control complex provides the logic, memory, and processing for call setup, call supervision, and call disconnection.

What Is a Key System?

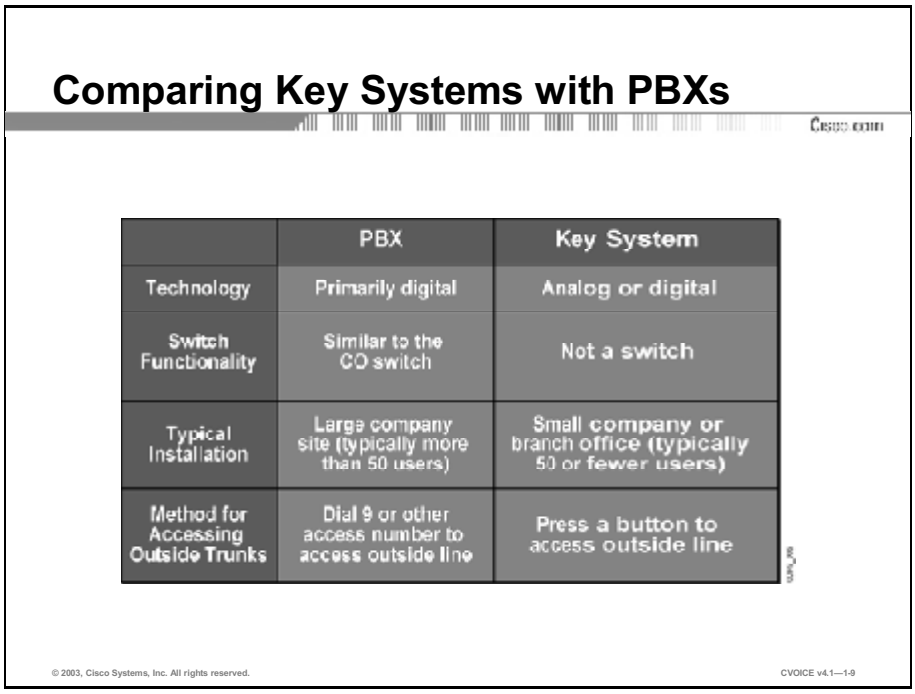


Small organizations and branch offices often use a key telephone system because a PBX offers functionality and extra features that they may not require. For example, a key system offers small businesses distributed answering from any telephone, unlike the central answering position required for a PBX.

Today, key telephone systems are either analog or digital and are microprocessor-based. Key systems are typically used in offices with 30 to 40 users, but can be scaled to support over 100 users.

A key system has three major components:

- **Key service unit:** A key service unit (KSU) holds the system switching components, power, intercom, line and station cards, and the system logic.
- **System software:** System software provides the operating system and calling-feature software.
- **Telephones (instruments or handsets):** Telephones allow the user to choose a free line and dial out, usually by pressing a button on the telephone.



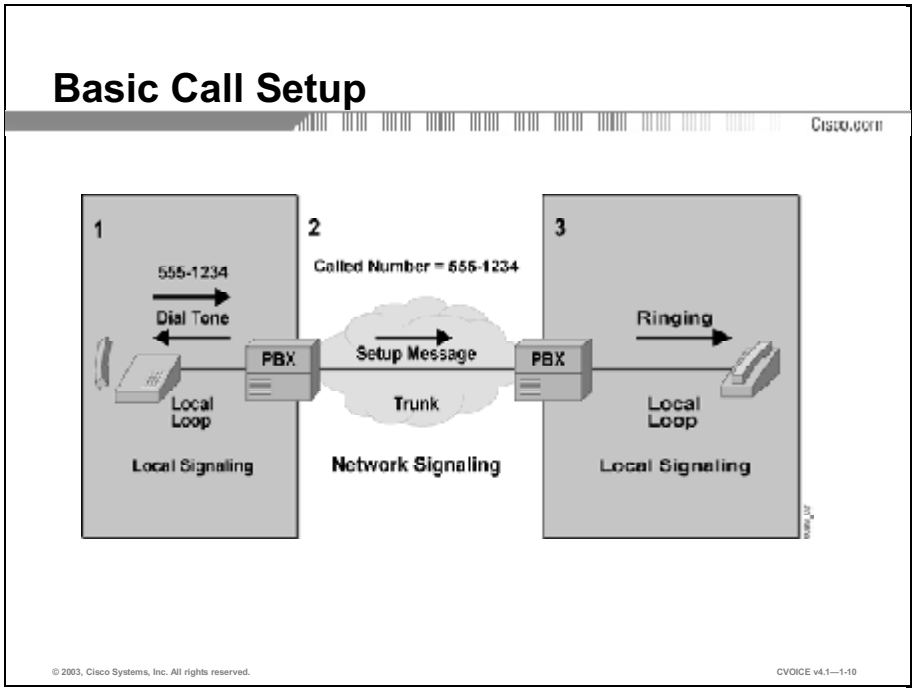
Larger companies use proprietary telephone networks with PBXs. In a key telephone system, each telephone has multiple line appearances that allow users to access outside lines to their CO. When a call comes into the company, a line or a key lights up on the telephone and indicates that a particular line is in use. Users can call another extension or let another person know where to pick up a call by using an intercom function, such as an overhead paging system or speakerphone.

Key telephone system functionality has evolved over time to include a class called hybrid telephone systems. The hybrid system adds many features that were previously available only in PBXs. There is no single definition of the functions and features that are classified as a hybrid system because all vendors provide a mix that they believe gives them a competitive advantage.

The main difference between a key telephone system and a hybrid telephone system is whether a single-line telephone can access a single CO local loop or trunk (key telephone system) only, or whether the single-line telephone can access a pool of CO local loops or trunks (hybrid telephone system).

Call Signaling

Call signaling, in its most basic form, is the capacity of a user to communicate a need for service to a network. The call-signaling process requires the ability to detect a request for and termination of service, send addressing information, and provide progress reports to the initiating party. This functionality corresponds to the three call-signaling types discussed in this topic: supervisory, address, and informational signaling.



The figure shows the three major steps in an end-to-end call. These steps include:

Step 1 Local signaling—originating side

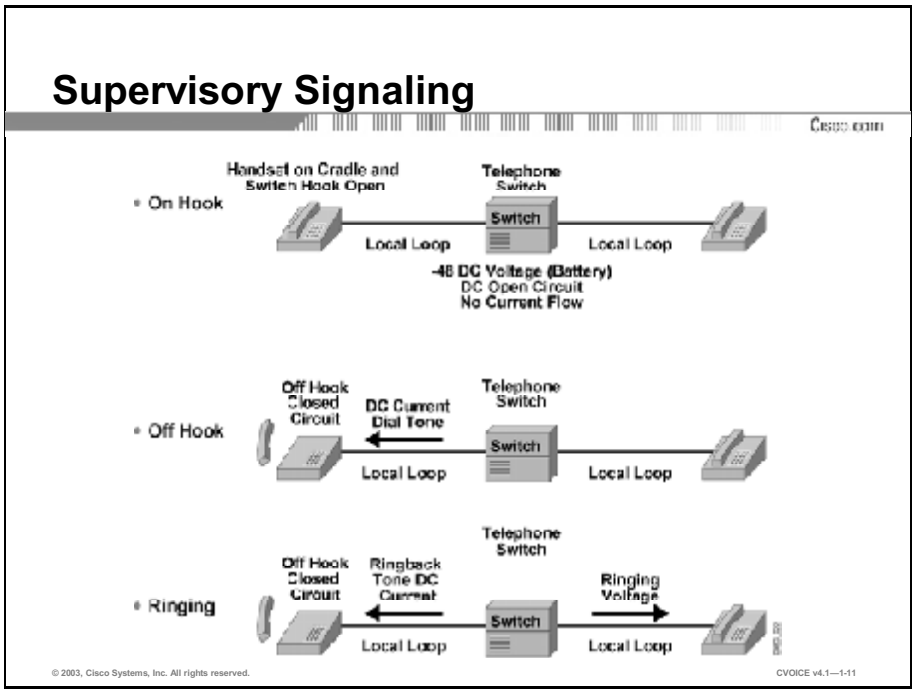
The user signals the switch by going off hook and sending dialed digits through the local loop.

Step 2 Network signaling

The switch makes a routing decision and signals the next, or terminating, switch through the use of setup messages sent across a trunk.

Step 3 Local signaling—terminating side

The terminating switch signals the call recipient by sending ringing voltage through the local loop to the recipient telephone.



A subscriber and telephone company notify each other of call status with audible tones and an exchange of electrical current. This exchange of information is called supervisory signaling.

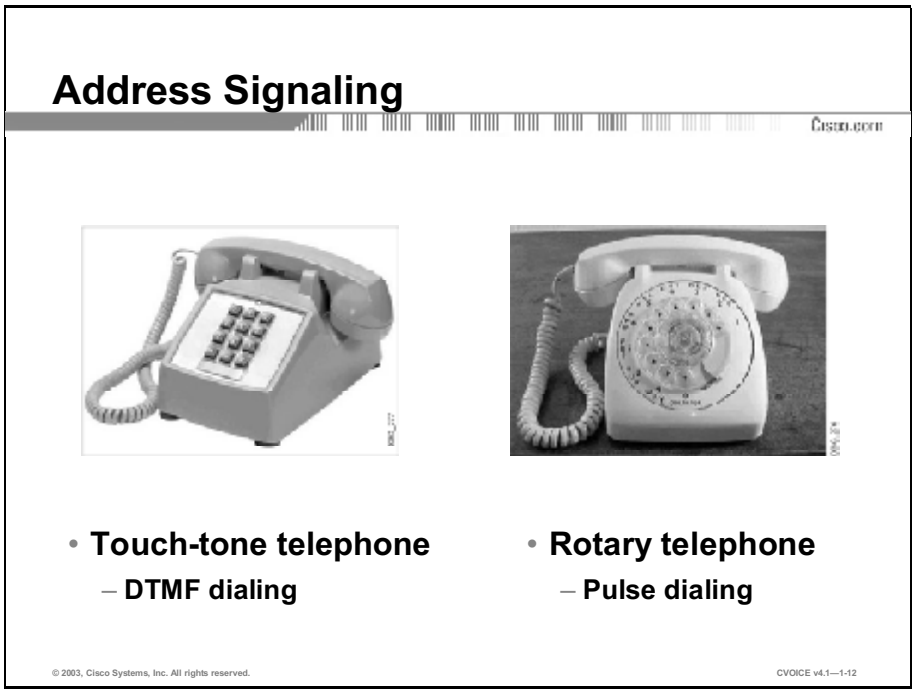
There are three different types of supervisory signaling:

- **On hook:** When the handset rests on the cradle, the circuit is on hook. The switch prevents current from flowing through the telephone. Regardless of the signaling type, a circuit goes on hook when the handset is placed on the telephone cradle and the switch hook is toggled to an open state. This prevents the current from flowing through the telephone. Only the ringer is active when the telephone is in this position.

- **Off hook:** When the handset is removed from the telephone cradle, the circuit is off hook. The switch hook toggles to a closed state, causing circuit current to flow through the electrical loop. The current notifies the telephone company equipment that someone is requesting to place a telephone call. When the telephone network senses the off hook connection by the flow of current, it provides a signal in the form of a dial tone to indicate that it is ready.

- **Ringing:** When a subscriber makes a call, the telephone sends voltage to the ringer to notify the other subscriber of an inbound call. The telephone company also sends a ringback tone to the caller alerting the caller that it is sending ringing voltage to the recipient telephone. Although the ringback tone sounds similar to ringing, it is a call progress tone and not part of supervisory signaling.

Note	The ringing tone in the United States is 2 seconds of tone followed by 4 seconds of silence. Europe uses a double ring followed by 2 seconds of silence.

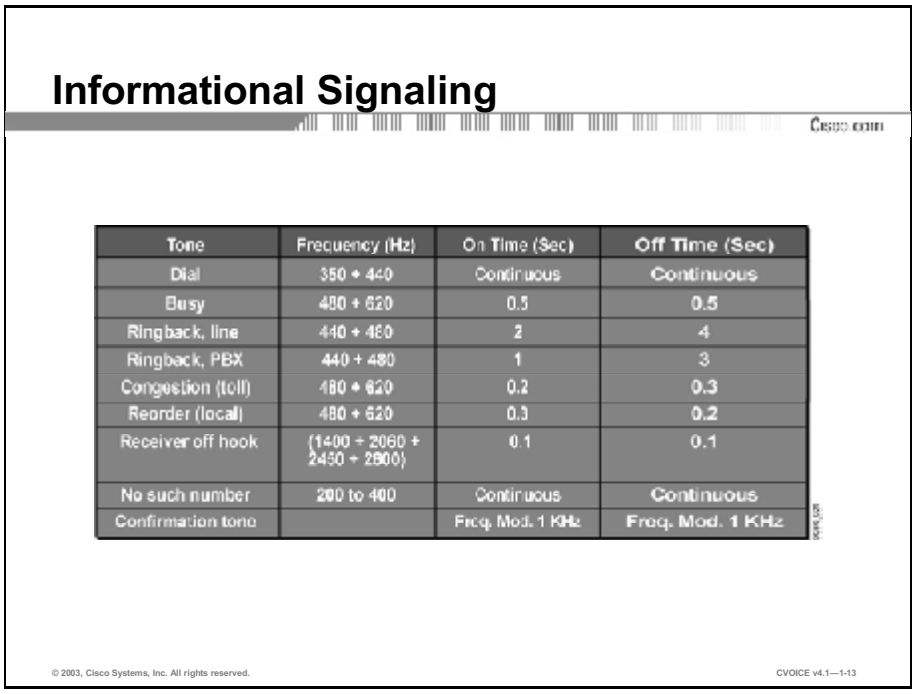


There are two types of telephones—a rotary-dial telephone and a push-button (touch-tone) telephone. These telephones use two different types of address signaling to notify the telephone company where a subscriber is calling:

- **Dual tone multifrequency:** Each button on the keypad of a touch-tone pad or push-button telephone is associated with a set of high and low frequencies. On the keypad, each row of keys is identified by a low-frequency tone and each column is associated with a high-frequency tone. The combination of both tones notifies the telephone company of the number being called, hence the term *dual tone multifrequency* (DTMF).

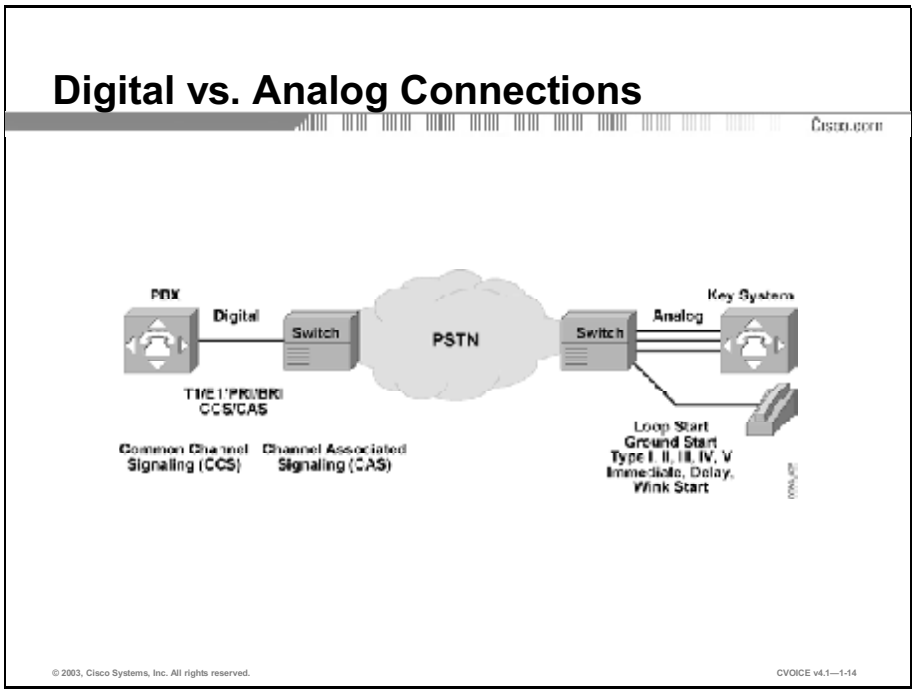
- **Pulse:** The large numeric dial-wheel on a rotary-dial telephone spins to send digits to place a call. These digits must be produced at a specific rate and within a certain level of tolerance. Each pulse consists of a "break" and a "make," which are achieved by opening and closing the local loop circuit. The break segment is the time during which the circuit is open. The make segment is the time during which the circuit is closed. The break/make cycle must correspond to a ratio of 60-percent break to 40-percent make.

A "governor" inside the dial controls the rate at which the digits are pulsed; for example, when a subscriber calls someone by dialing a digit on the rotary dial, a spring winds. When the dial is released, the spring rotates the dial back to its original position. While the spring rotates the dial back to its original position, a cam-driven switch opens and closes the connection to the telephone company. The number of consecutive opens and closes—or breaks and makes—represents the dialed digit.



Tone combinations indicate call progress and are used to notify subscribers of call status. Each combination of tones represents a different event in the call process. These events include:

- **Dial tone:** Indicates that the telephone company is ready to receive digits from the user telephone.
- **Busy:** Indicates that a call cannot be completed because the telephone at the remote end is already in use.
- **Ringback (normal or PBX):** Indicates that the telephone company is attempting to complete a call on behalf of a subscriber.
- **Congestion:** Indicates that congestion in the long distance telephone network is preventing a telephone call from being processed.
- **Reorder tone:** Indicates that all the local telephone circuits are busy, thus preventing a telephone call from being processed.
- **Receiver off hook:** Indicates that a receiver has been off hook for an extended period of time without placing a call.
- **No such number:** Indicates that a subscriber has placed a call to a nonexistent number.
- **Confirmation tone:** Indicates that the telephone company is attempting to complete a call.



Supervisory, addressing, and informational signaling must be carried across both analog and digital connections. Depending on the subscriber connection to the network, you must configure specific signaling to match the type of signaling required by the service provider.

Digital PBX connections to the network are common in many countries; they may be a T1 or E1 line carrying channel associated signaling (CAS) or a PRI using common channel signaling (CCS).

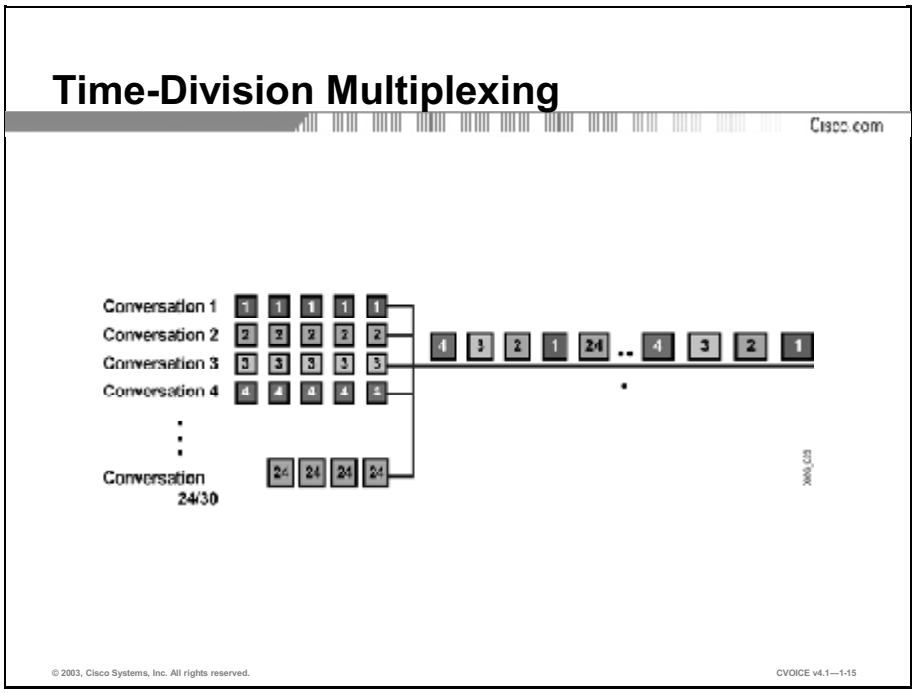
CAS is a signaling method that allows passing on-hook or off-hook status by setting bits that are associated with each specific voice channel. These bits are carried in band for T1 and out of band for E1.

An ISDN connection uses the D channel as the common channel to carry signaling messages for all other channels. CCS carries the signaling out of band, meaning that the signaling and the voice path do not share the same channel.

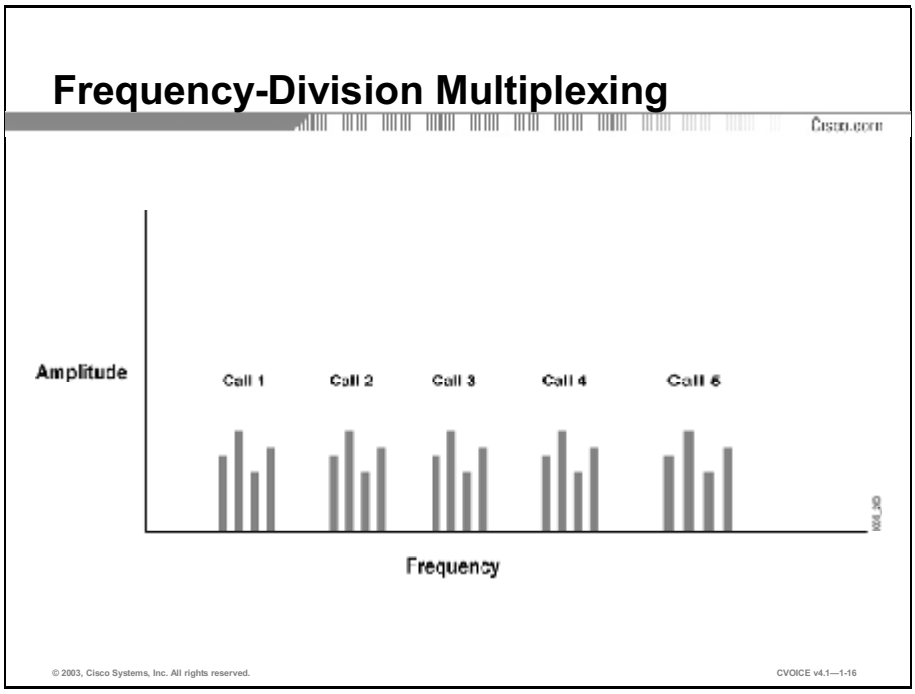
Analog interfaces require configuration of a specific signaling type to match the provider requirement. For interfaces that connect to the PSTN or to a telephone or similar edge device, the signaling is configured for either loop start or ground start. For analog trunk interfaces that connect two PBXs to each other, or a PBX to a CO switch, the signaling is either Wink Start, immediate start, or delay start with the signaling type set to 1, 2, 3, 4, or 5.

Multiplexing Techniques

A two-wire analog local loop typically carries one call at a time. To make better use of wiring facilities, different multiplexing techniques have been implemented to enable two-wire or four-wire connections to carry multiple conversations at the same time. This topic discusses two of these multiplexing techniques.



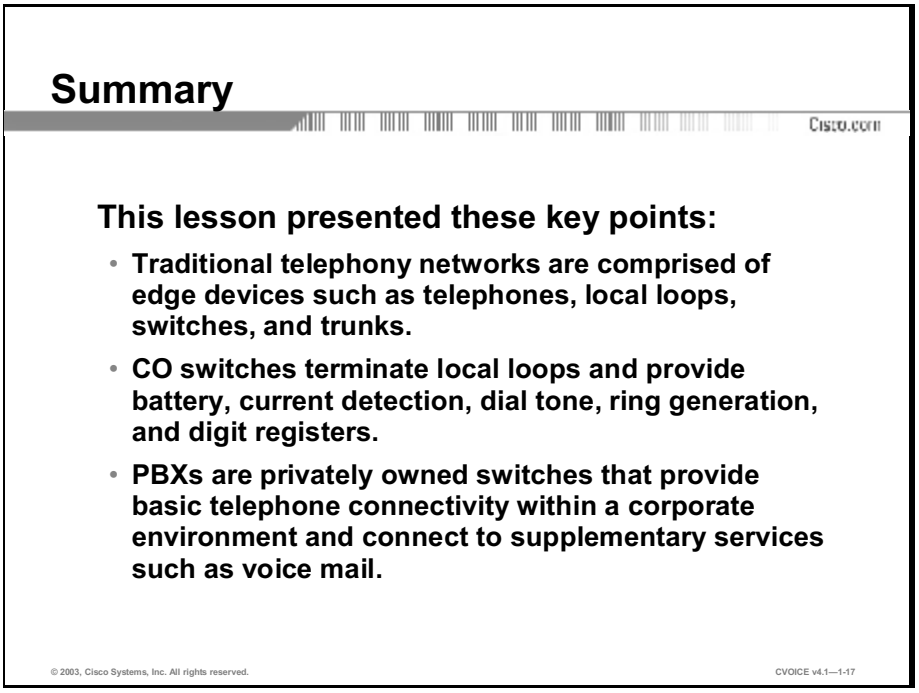
Time-division multiplexing (TDM) is used extensively in telephony networks to carry multiple conversations concurrently across a four-wire path. TDM involves simultaneously transmitting multiple separate voice signals over one communications medium by quickly interleaving pieces of each signal, one after another. Information from each data channel is allocated bandwidth based on preassigned time slots, regardless of whether there is data to transmit.

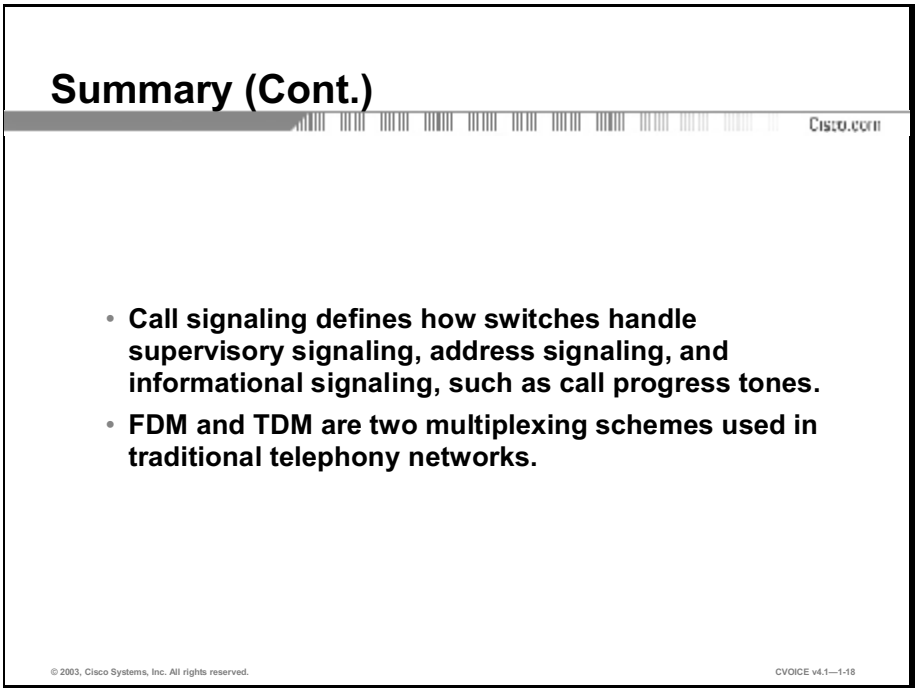


Frequency-division multiplexing (FDM) involves carrying multiple voice signals by allocating an individual frequency range to each call. FDM is typically used in analog connections, although its functionality is similar to that of TDM in digital connections. FDM is often used in cable or digital subscriber line (DSL) connections to allow the simultaneous use of multiple channels over the same wire.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Traditional Telephony
- Packetized Telephony Networks lesson

References

For additional information, refer to these resources:

- “Voice Network Signaling and Control”
  http://www.cisco.com/warp/public/788/signalling/net_signal_control.html

Quiz: Traditional Telephony

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the components and functionality of traditional telephony networks
- Explain how central office switches process telephone calls
- Identify types of private switching systems used in traditional telephony networks and list the main features of each
- Describe the three types of signaling in traditional telephony networks and identify how each is used
- Describe two methods used to multiplex voice in traditional telephony networks

Instructions

Answer these questions:

Q1) Match the component of a telephony network with the function it performs.

A) edge device

B) local loop

C) private or CO switch

D) trunk

_____ 1. handles signaling, call routing, call setup and call teardown

_____ 2. provides a path between two switches

_____ 3. connects to the PSTN

_____ 4. interfaces to the telephone company network

Q2) Which type of trunk connects two local telephone company COs?

A) tie trunk

B) CO trunk

C) interoffice trunk

D) all of the above

Q3) Two CO switch components that make a telephone work include a battery, ring generator, dial tone generator, _____, and _____. (Choose two.)

A) tandem switch

B) current detector

C) terminal interface

D) control complex

E) digit register

Q4) Dial tone is generated when the _____.

A) user dials a number

B) flow of current is interrupted

C) DTMF tones are detected

D) dial register is ready

Q5) The difference between a PBX and a key system is that a _____.

A) key system handles more calls

B) key system is digital only

C) key system is not a switch

D) key system is analog only

Q6) Which three of the following are components of a key system? (Choose three.)

A) terminal interface

B) key service unit

C) telephones

D) control complex

E) switching network

F) system software

Q7) Match the type of signaling to its description.

A) supervisory signaling

B) informational signaling

C) address signaling

_____ 1. is a type of signaling that uses either pulse or DTMF

_____ 2. provides call progress indicators to the initiator of a call

_____ 3. is a type of signaling that monitors on hook/off hook transitions and provides call notification

Q8) CAS passes signaling _____.

A) in the same channel as voice for T1

B) in the D channel

C) using frequency-division multiplexing

D) using DTMF frequencies

Q9) Which multiplexing process is used by TDM?

A) Timeslots are assigned to different channels, regardless of whether there is data to transmit.

B) Timeslots are assigned to different channels depending on which traffic has a higher priority at that time.

C) All timeslots are used by the channel that is transmitting data at that time.

D) Timeslots are assigned to the channel that starts transmitting first and used by the other channels as they become available.

Q10) DSL is an example of _____.

A) frequency-division multiplexing

B) phase-division multiplexing

C) time-division multiplexing

D) statistical time-division multiplexing

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Packetized Telephony Networks

Overview

This lesson investigates the driving forces behind converging networks, the components of Packet Telephony Networks, the traffic characteristics of packet telephony, and the control of call volume in the network.

Importance

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. Multiplexing voice traffic with data traffic reduces the number of costly circuits dedicated to servicing voice applications.

As demand for voice services expands, it is important to understand the different requirements of voice and data traffic. Previously, voice and data networks were separate and could not impact each other. Today, it is necessary to determine the protocols that are available to control voice calls and ensure that data flows are not negatively impacted.

Objectives

Upon completing this lesson, you will be able to:

- List five benefits of Packet Telephony Networks compared to circuit-switched networks
- Briefly describe three mechanisms of call control that are used in packet telephony
- Compare the gateway functions and signaling processes in centralized and distributed call control models
- List seven basic components of a packet voice network
- Identify a solution for transmitting real-time traffic, such as Voice over IP, on a best-effort delivery network, such as IP

Learner Skills and Knowledge

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

- General knowledge of telephony technology, including customer premises equipment (CPE) and the public switched telephone network (PSTN)
- General knowledge of networking terminology and IP network concepts

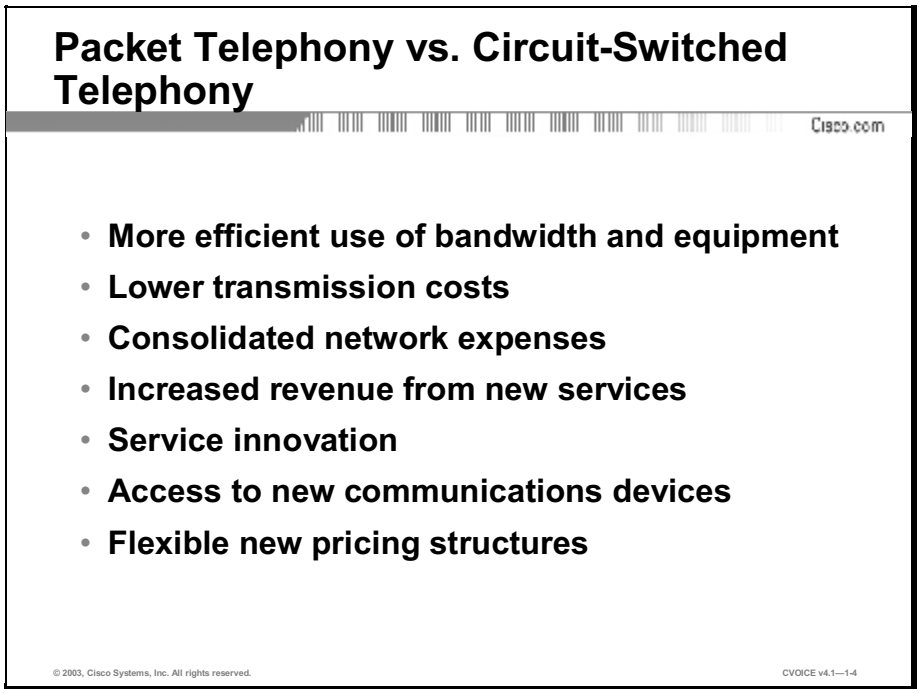
Outline

This lesson includes these topics:

- Overview
- Benefits of Packet Telephony Networks
- Call Control
- Distributed vs. Centralized Call Control
- Packet Telephony Components
- Best-Effort Delivery of Real-Time Traffic
- Summary
- Assessment (Quiz): Packetized Telephony Networks

Benefits of Packet Telephony Networks

Traditionally, the potential savings on long-distance costs was the driving force behind the migration to converged voice and data networks. The cost of long-distance calls has dropped in recent years and other factors have come to the forefront as benefits of converged networks. This topic describes some of these benefits.



The benefits of packet telephony versus circuit-switched telephony are as follows:

- **More efficient use of bandwidth and equipment:** Traditional telephony networks use a 64-kbps channel for every voice call. Packet telephony shares bandwidth among multiple logical connections and offloads traffic volume from existing voice switches.

- **Lower costs for telephony network transmission:** 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 represents substantial savings on capital equipment and operations costs.

- **Consolidated voice and data network expenses:** Data networks that function as separate networks to voice networks become major traffic carriers. The underlying voice networks are converted to utilize the packet-switched architecture to create a single integrated communications network with a common switching and transmission system. The benefit is significant cost savings on network equipment and operations.

- **Increased revenues from new services:** Packet telephony enables new integrated services, such as broadcast-quality audio, unified messaging, and real-time voice and/or data collaboration. These services increase employee productivity and profit margins well above those of basic voice services. In addition, these services enable companies and service providers to differentiate themselves and improve their market position.

- **Greater innovation in services:** Unified communications use the IP infrastructure to consolidate communication methods that were previously independent; for example, fax, voice mail, e-mail, wire-line telephones, cellular telephones, and the web. The IP infrastructure provides users with a common method to access messages and initiate real-time communications—independent of time, location, or device.

- **Access to new communications devices:** Packet technology can reach devices that are largely inaccessible to the time-division multiplexing (TDM) infrastructures of today. Examples of such devices are computers, wireless devices, household appliances, personal digital assistants, and cable set-top boxes. Intelligent access to such devices enables companies and service providers to increase the volume of communications they deliver, the breadth of services they offer, and the number of subscribers they serve. Packet technology, therefore, enables companies to market new devices, including videophones, multimedia terminals, and advanced IP Phones.

- **Flexible new pricing structures:** Companies and service providers with packet-switched networks can transform their service and pricing models. Because network bandwidth can be dynamically allocated, network usage no longer needs to be measured in minutes or distance. Dynamic allocation gives service providers the flexibility to meet the needs of their customers in ways that bring them the greatest benefits.

Although packet technology has clear benefits, you should carefully consider the following points before migrating to this technology:

- Return on investment (ROI), when based on the new system features, can be difficult to prove

- Generally, voice and data staffs do not speak the same language

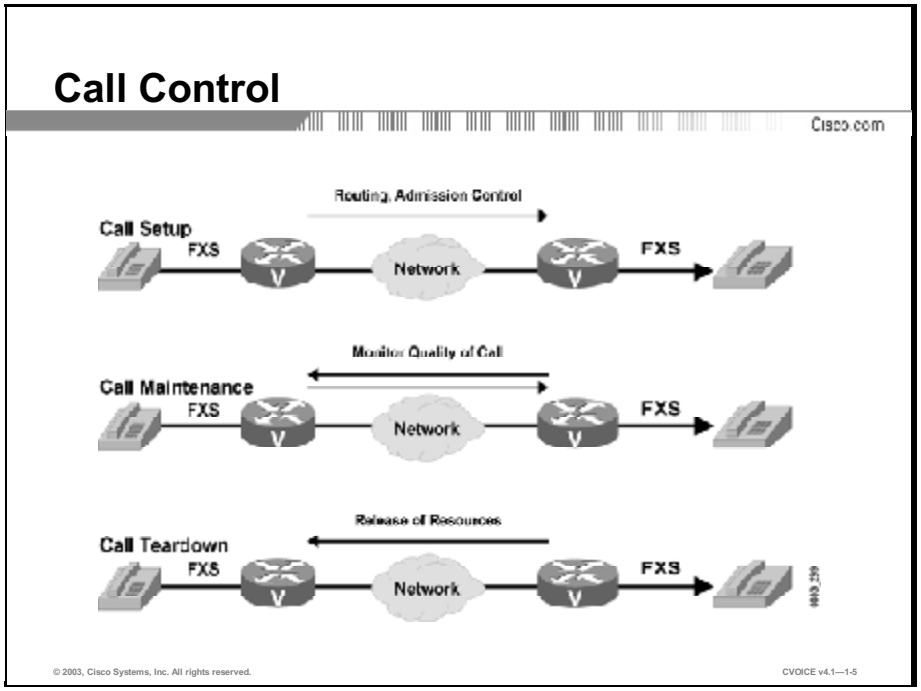
- Current voice telephony components have not yet fully depreciated

- Potential upgrade costs will override potential savings benefits

- The long-distance carrier may be unwilling to offer price breaks based on digital technology

Call Control

Call control allows users to establish, maintain, and disconnect a voice flow across a network. This topic describes call control services.



Although different protocols address call control in different ways, they all provide a common set of services. The following are basic components of call control:

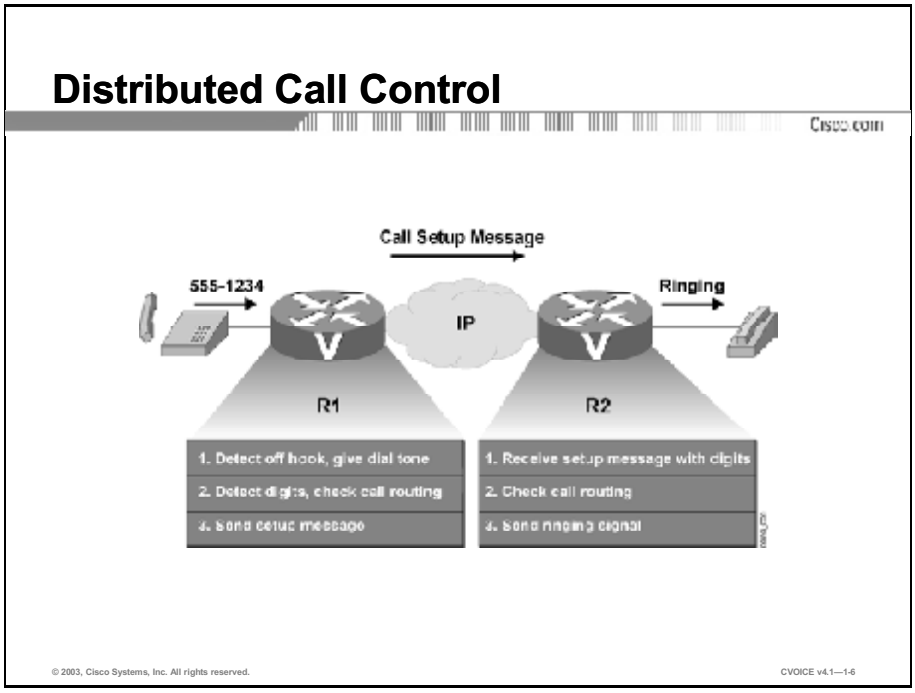
- **Call setup:** Checks call-routing configuration to determine the destination of a call. The configuration specifies the bandwidth requirements for the call. When the bandwidth requirements are known, Call Admission Control (CAC) determines if sufficient bandwidth is available to support the call. If bandwidth is available, call setup generates a setup message and sends it to the destination. If bandwidth is not available, call setup notifies the initiator by presenting a busy signal. Different call control protocols, such as H.323, Media Gateway Control Protocol (MGCP), and session initiation protocol (SIP), define different sets of messages to be exchanged during setup.

- **Call maintenance:** Tracks packet count, packet loss, and interarrival jitter or delay when the call is set up. Information passes to the voice-enabled devices to determine if connection quality is good or if it has deteriorated to the point where the call should be dropped.

- **Call teardown:** Notifies voice-enabled devices to free resources and make them available for the next call when either side terminates a call.

Distributed vs. Centralized Call Control

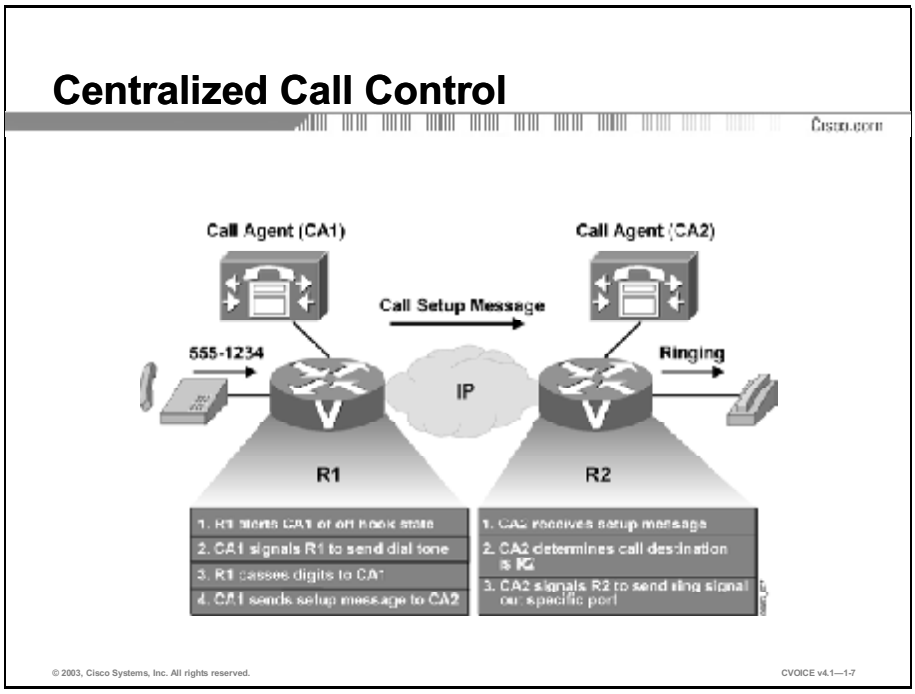
This topic compares distributed and centralized call control.



This figure shows an environment where call control is handled by multiple components in the network. Distributed call control is possible where the voice-capable device is configured to support call control directly. This is the case with a voice gateway when protocols, such as H.323 or SIP, are enabled on the device.

Distributed call control enables the gateway to perform the following procedure:

1. Recognize the request for service
2. Process dialed digits
3. Route the call
4. Supervise the call
5. Terminate the call



Centralized call control allows an external device (call agent) to handle the signaling and call processing, leaving the gateway to translate audio signals into voice packets after call setup. The call agent is responsible for all aspects of signaling, thus instructing the gateways to send specific signals at specific times.

When the call is set up:

- The voice path runs directly between the two gateways and does not involve the call agent.
- When either side terminates the call, the call agent signals the gateways to release resources and wait for another call.

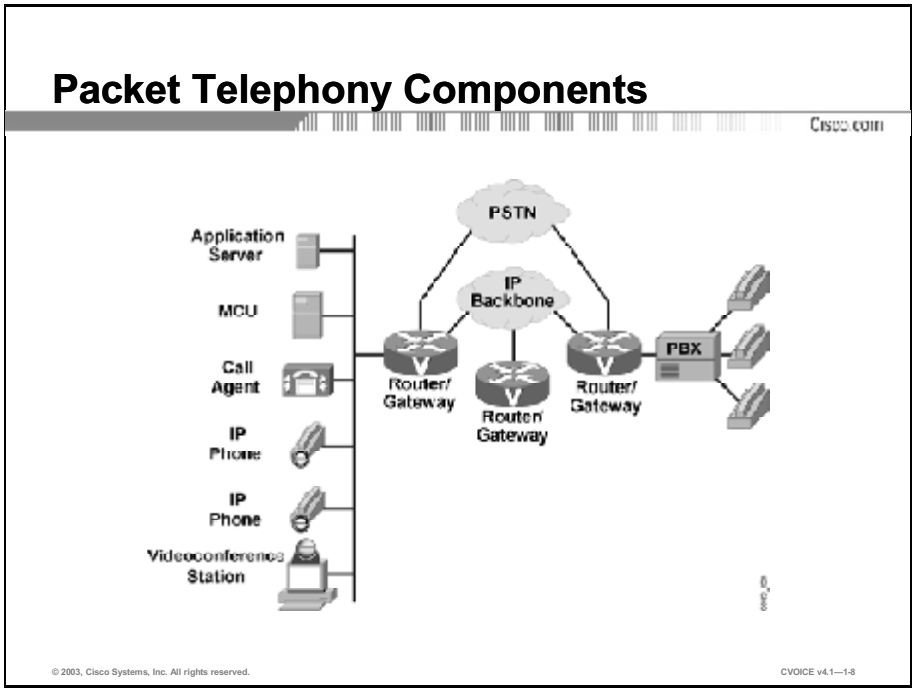
The use of centralized call control devices is beneficial in several ways:

- It centralizes the configuration for call routing and CAC. In a large voice environment, centralization can be extremely beneficial.
- The call agent is the only device that needs the intelligence to understand and participate in call control functions. These call control functions enable the customer to purchase less expensive voice-gateway devices and point to a single device to handle call control.

MGCP is one example of a centralized call control model.

Packet Telephony Components

This topic introduces the basic components of a packet voice network.



The basic components of a packet voice network include the following:

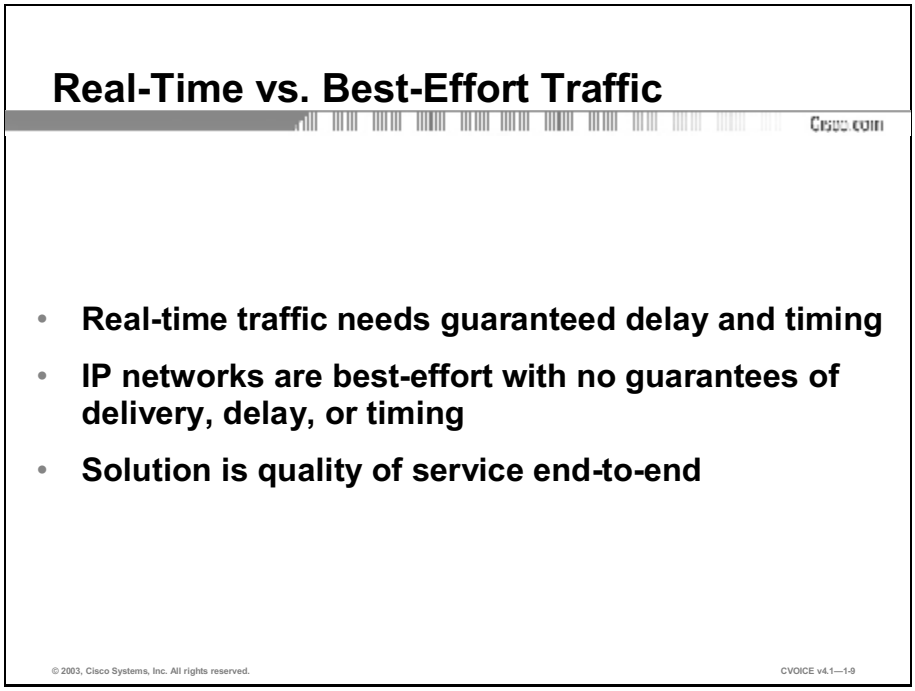
- **IP Phones:** Provide IP voice to the desktop.
- **Gatekeeper:** Provides CAC, bandwidth control and management, and address translation.
- **Gateway:** Provides translation between Voice over IP (VoIP) and non-VoIP networks, such as the public switched telephone network (PSTN). It also provides physical access for local analog and digital voice devices, such as telephones, fax machines, key sets, and PBXs.
- **Multipoint control unit (MCU):** Provides real-time connectivity for participants in multiple locations to attend the same videoconference or meeting.
- **Call agent:** Provides call control for IP Phones, CAC, bandwidth control and management, and address translation.
- **Application servers:** Provide services such as voice mail, unified messaging, and Cisco CallManager Attendant Console.

- **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.

Best-Effort Delivery of Real-Time Traffic

Voice and data can share the same medium; however, their traffic characteristics differ widely: voice is real-time traffic and data is typically sent as best-effort traffic. This topic compares real-time requirements versus best-effort delivery.



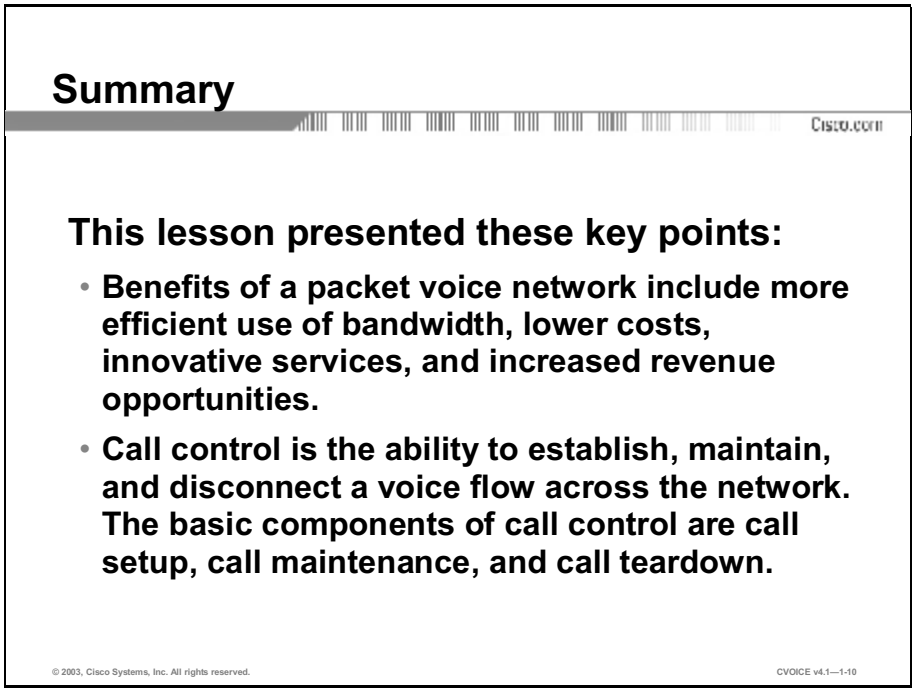
Traditional telephony networks were designed for real-time voice transmission and therefore, cater to the need for a constant voice flow over the connection. Resources are reserved end to end on a per-call basis and are not released until the call is terminated. These resources guarantee that voice flows in an orderly manner. Good voice quality depends on the capacity of the network to deliver voice with guaranteed delay and timing—the requirement for delivery of real-time traffic.

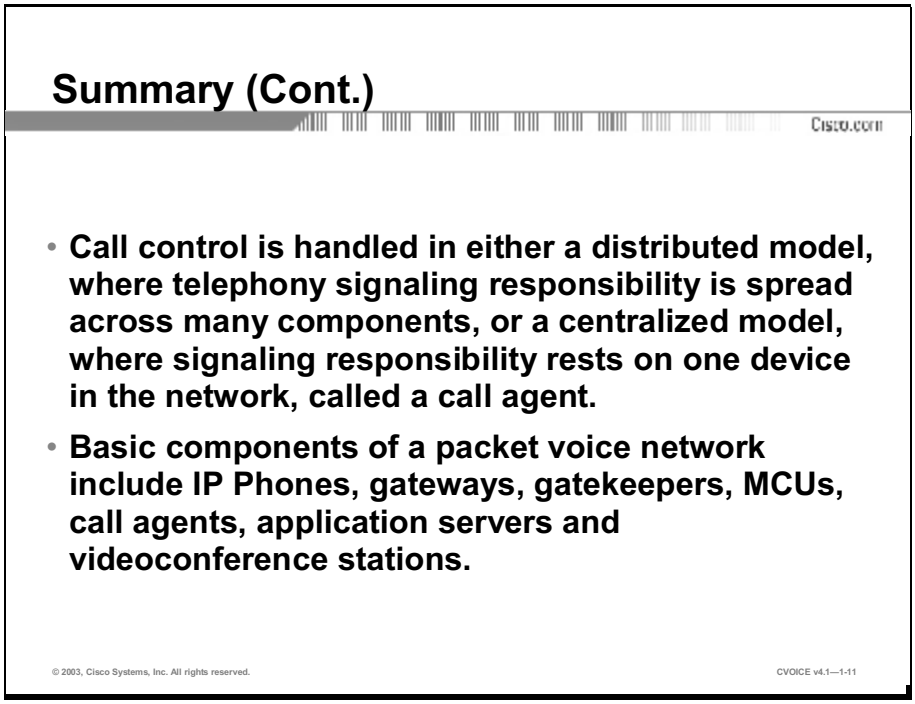
Traditional data networks were designed for best-effort packet transmission; packet telephony networks transmit with no guarantee of delivery, delay, or timing. Data handling is effective in this scenario because upper-layer protocols, such as TCP, provide for reliable—although untimely—packet transmission. TCP trades delay for reliability. Data can typically tolerate a certain amount of delay and is not affected by interpacket jitter.

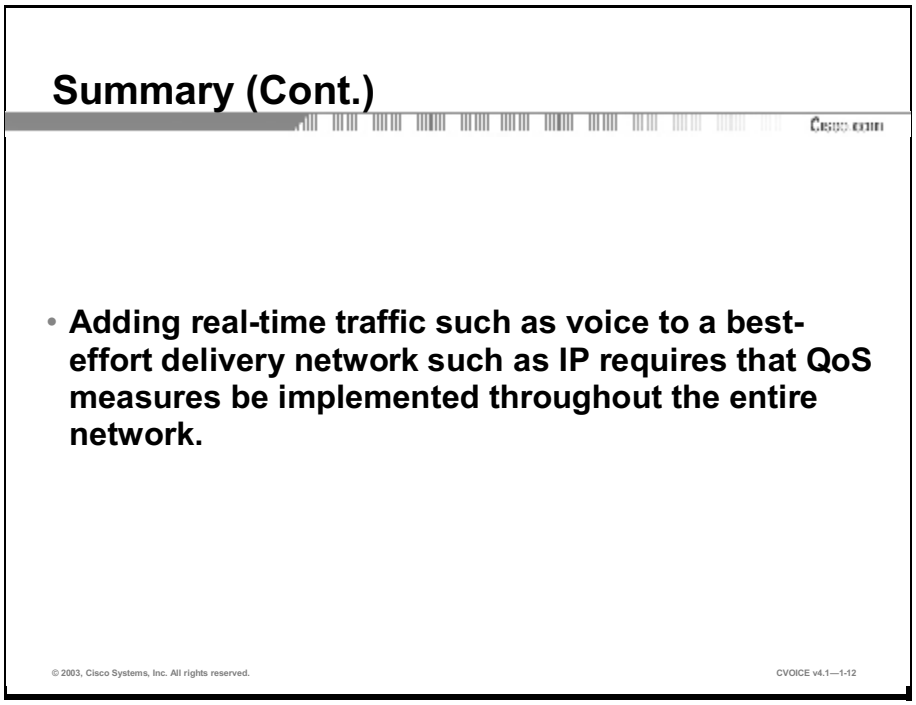
A well-engineered, end-to-end network is required when converging delay-sensitive traffic, such as VoIP, with best-effort data traffic. Fine-tuning the network to adequately support VoIP involves a series of protocols and features to improve quality of service (QoS). Because the IP network is, by default, best-effort, steps must be taken to ensure proper behavior of both the real-time and best-effort traffic. Packet telephony networks succeed, in large part, based on the QoS parameters that are implemented network-wide.

Summary

This topic summarizes the key points discussed in this lesson.







Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Packetized Telephony Networks
- IP Telephony Applications lesson

References

For additional information, refer to these resources:

- "Extending Enterprise Productivity with Converged IP-Based Cisco Solutions" http://www.cisco.com/warp/public/cc/so/neso/vvda/avvid/avid_pl.htm

Quiz: Packetized Telephony Networks

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- List five benefits of Packet Telephony Networks compared to circuit-switched networks
- Briefly describe three mechanisms of call control that are used in packet telephony
- Compare the gateway functions and signaling processes in centralized and distributed call-control models
- List seven basic components of a packet voice network
- Identify a solution for transmitting real-time traffic, such as VoIP, on a best-effort delivery network, such as IP

Instructions

Answer these questions:

Q1) Which of the following is NOT a benefit of packet voice networks?

A) consolidated voice and data network expenses

B) guaranteed delivery of digital voice

C) greater innovation in services

D) more efficient use of bandwidth and equipment

Q2) What is the main drawback of migrating to packet technology?

A) Upgrade cost may override potential cost savings.

B) New devices may not be compatible with the existing PBX.

C) Unified communications may overload the network.

D) Voice transmission cost may increase.

Q3) Which function is NOT performed by call control?

A) establishing a call

B) maintaining a call

C) routing a call

D) disconnecting a call

Q4) Which two functions are performed by the call setup component of call control? (Choose two.)

A) monitors the quality of the connection

B) determines the destination of the call

C) tracks packet count and packet loss

D) notifies voice-enabled devices to make resources available for next call

E) sends the call initiator a busy signal if sufficient bandwidth is not available

Q5) Which two protocols are examples of distributed call control? (Choose two.)

A) MGCP

B) H.323

C) SIP

D) Megaco

Q6) In the centralized call control model, signaling is performed by the _____.

A) gateway

B) gatekeeper

C) MCU

D) call agent

Q7) The three purposes of a gatekeeper include _____. (Choose three.)

A) CAC

B) access to the PSTN

C) bandwidth control and management

D) billing and accounting

E) address translation

Q8) 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

Q9) Two guarantees of real-time traffic include _____. (Choose two.)

A) delay

B) routing

C) decibels

D) timing

Q10) Traditional data networks were designed for _____.

A) real-time packet transmission

B) guaranteed delivery

C) guaranteed timing

D) best-effort packet delivery

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

IP Telephony Applications

Overview

This lesson provides an overview of analog, digital, and Ethernet voice interfaces. It demonstrates campus, enterprise, and service provider voice-network topologies.

Importance

As customers migrate their voice networks, they face a myriad of choices regarding interface types, components, and topologies. A good network design incorporates solutions for current requirements and room for future growth. It is important to understand how voice interfaces with a network, and how the components fit together to provide service in any environment.

Objectives

Upon completing this lesson, you will be able to:

- Describe the three basic analog interfaces and the telephony devices that they connect
- Describe the three basic digital interfaces and the type of signaling that each interface supports
- Describe the three physical connectivity options for IP Phones and explain the functioning of the Cisco IP Phone
- List five basic components of an integrated voice and data campus LAN network
- Explain the difference between distributed and centralized enterprise environments and list five main components of each enterprise network type
- List four capabilities that allow service provider networks to offer more efficient, less expensive alternatives to the public switched telephone network

Learner Skills and Knowledge

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

- General knowledge of telephony technology, including customer premises equipment (CPE) and the public switched telephone network (PSTN)

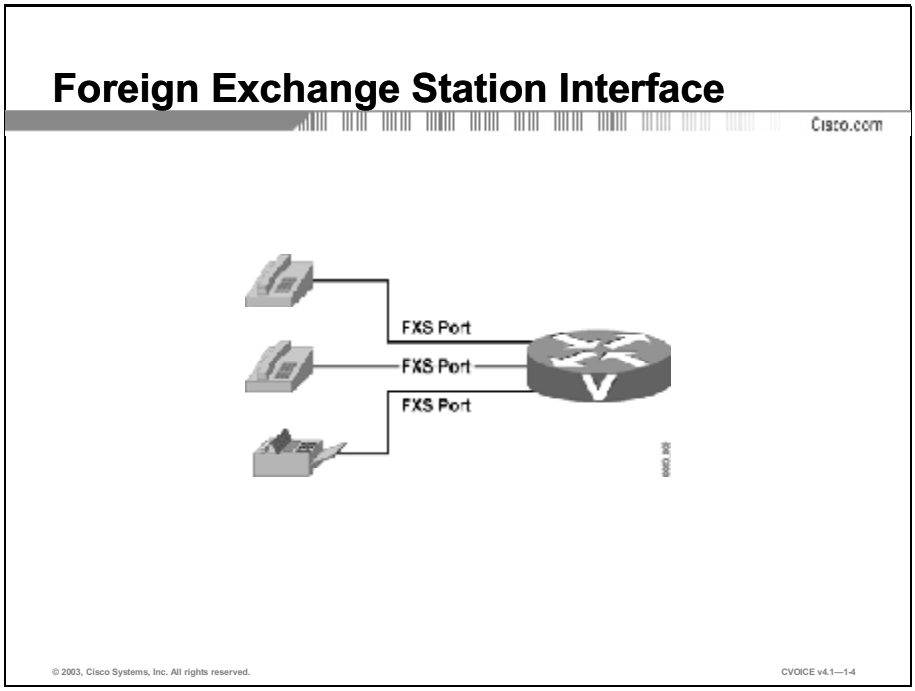
Outline

This lesson includes these topics:

- Overview
- Analog Interfaces
- Digital Interfaces
- IP Phones
- Campus LAN Environment
- Enterprise Environment
- Service Provider Environment
- Summary
- Assessment (Quiz): IP Telephony Applications

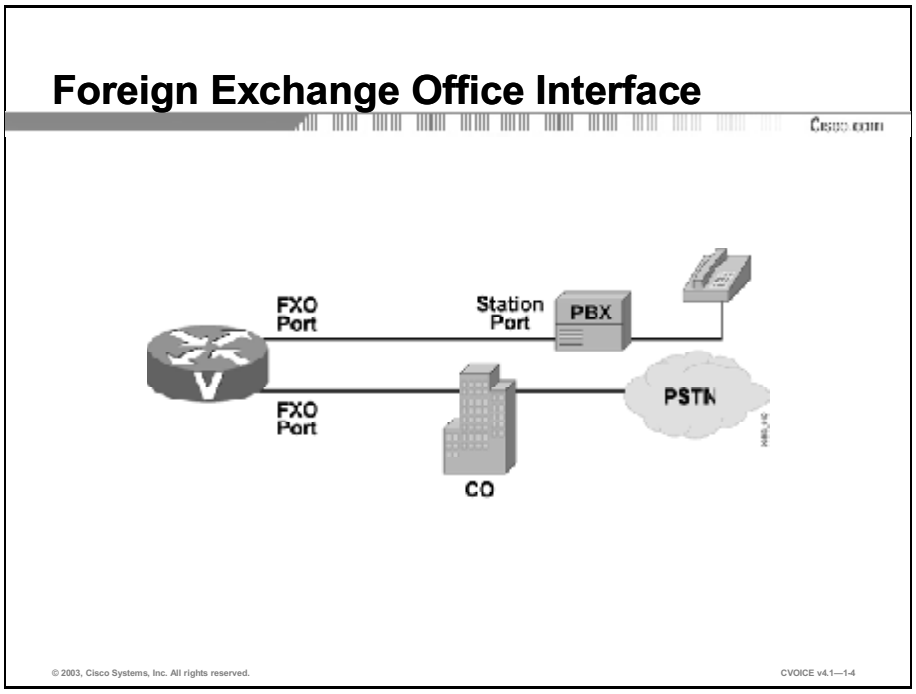
Analog Interfaces

This topic defines three analog interfaces: Foreign Exchange Station (FXS), Foreign Exchange Office (FXO), and ear and mouth (E&M). It also discusses how each of these interfaces is used.



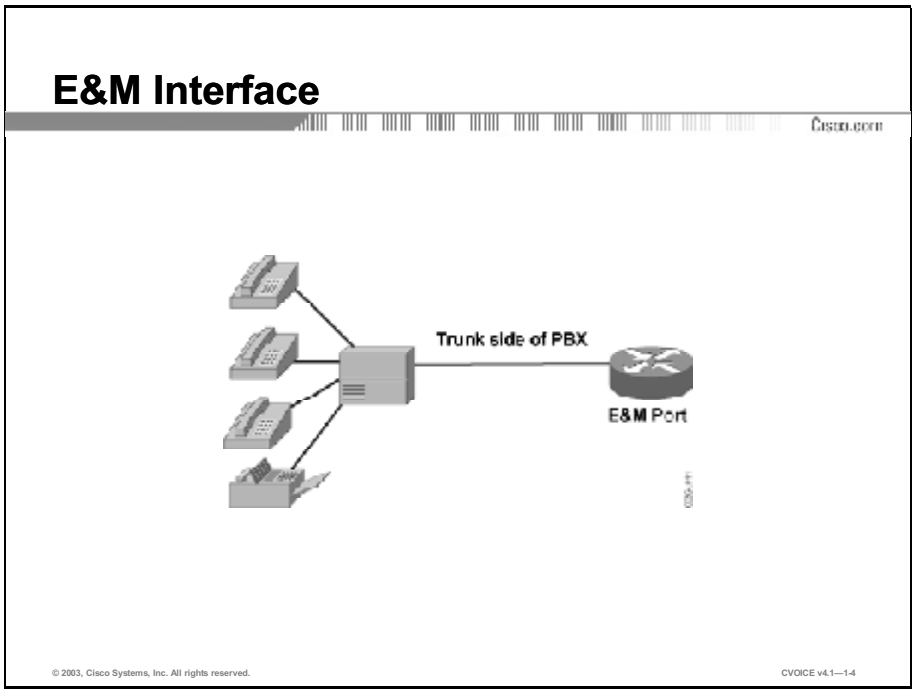
This figure depicts an FXS interface. The FXS interface provides a direct connection to an analog telephone, a fax machine, or a similar device. From a telephone perspective, the FXS interface functions like a switch; therefore, it must supply line power, ring voltage, and dial tone.

The FXS interface contains the coder-decoder (codec), which converts the spoken analog voice wave into a digital format for processing by the voice-enabled device.



This figure depicts an FXO interface. The FXO interface allows an analog connection to be directed at the central office (CO) of a public switched telephone network (PSTN) or to a station interface on a PBX. The switch recognizes the FXO interface as a telephone because the interface plugs directly into the line side of the switch. The FXO interface provides either pulse or dual tone multifrequency (DTMF) digits for outbound dialing.

In PSTN terminology, an FXO-to-FXS connection is also referred to as a Foreign Exchange (FX) trunk. An FX trunk is a CO trunk that has access to a distant CO. Because this connection is FXS at one end and FXO at the other end, it acts as a long-distance extension of a local phone line. In this instance, a local user can pick up the telephone and get a dial tone from a foreign city. Users in the foreign city can dial a local number and have the call connect to the user in the local city.

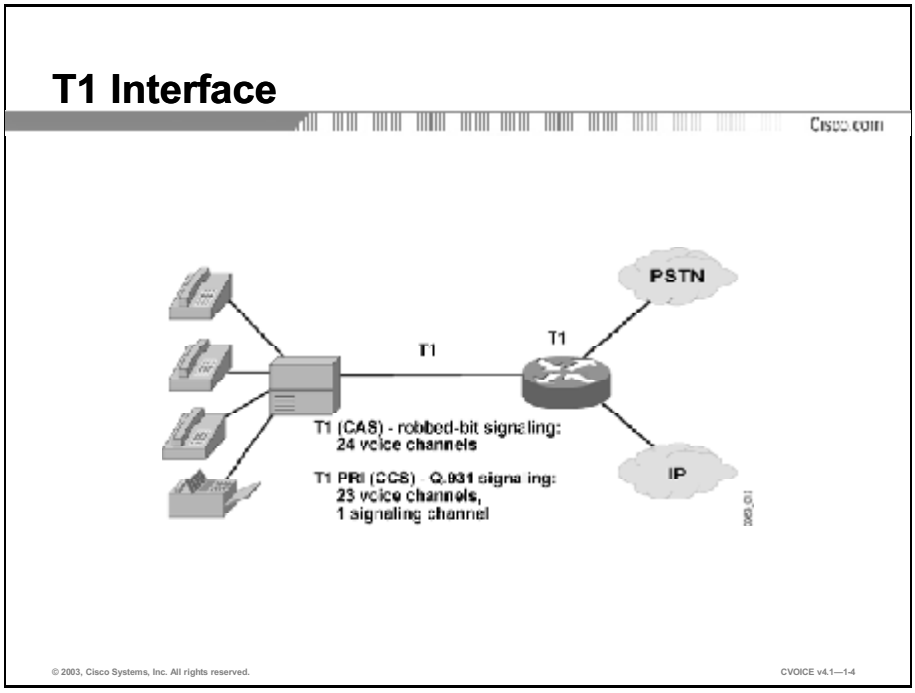


This figure depicts an ear and mouth (E&M) interface. The E&M interface provides signaling for analog trunking. Analog trunk circuits connect automated systems (PBXs), and networks (COs.) E&M signaling is also referred to as “recEive and transMit,” but its origin comes from the term “earth and magneto.” Earth represents the electrical ground and magneto represents the electromagnet used to generate tone.

E&M signaling defines a trunk-circuit side and a signaling-unit side for each connection, similar to the DCE and DTE reference type. The PBX is usually the trunk-circuit side and the telco, CO, channel bank, or Cisco voice-enabled platform is the signaling-unit side.

Digital Interfaces

This topic describes the three basic digital voice interfaces: T1, E1, and BRI.



This figure depicts a T1 interface. In a corporate environment with a large volume of voice traffic, connections to the PSTN and to PBXs are primarily digital.

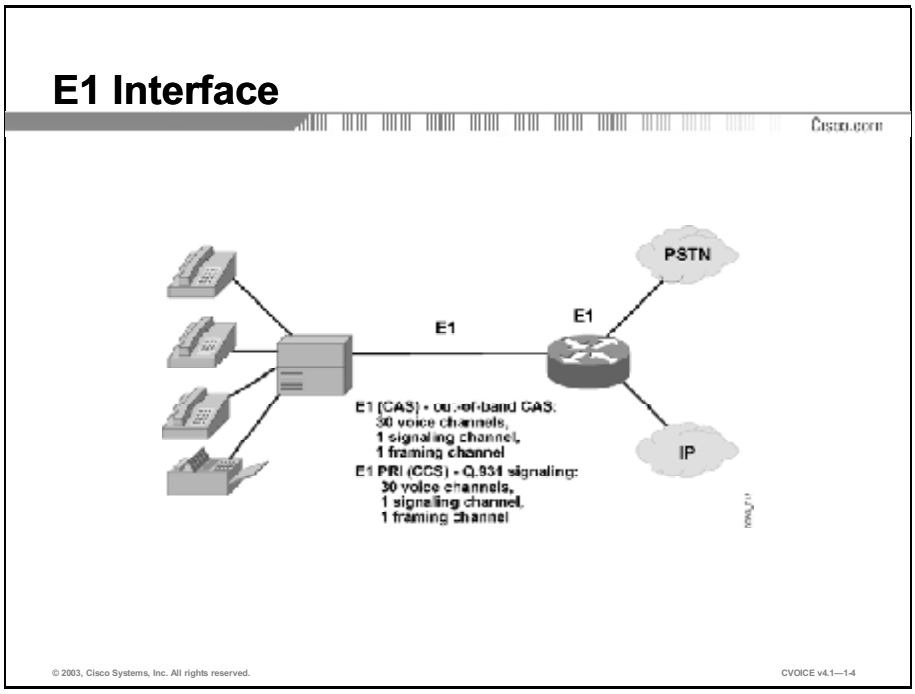
A T1 interface is a form of digital connection that can simultaneously carry up to 24 conversations using two wire pairs. When a T1 link operates in full-duplex mode, one wire pair sends and the other wire pair receives. The 24 channels are grouped together to form a frame. The frames are then grouped together into superframes (groups of 12 frames) or into extended superframes (groups of 24 frames).

The T1 interface carries either channel associated signaling (CAS) or common channel signaling (CCS). When a T1 interface uses CAS, the signaling robs a sampling bit for each channel to convey in band. When a T1 interface uses CCS, Q.931 signaling is used on a single channel, typically the last channel.

To configure CAS you must:

- Specify the type of signaling that the robbed bits carry; for example, E&M Wink Start. This signaling must match the PSTN requirements or the PBX configuration. This is considered in-band signaling because the signal shares the same channel as the voice.

- Configure the interface for PRI signaling. This level of configuration makes it possible to use channels 1 to 23 (called B channels) for voice traffic. Channel 24 (called the D channel) carries the Q.931 call-control signaling for call setup, maintenance, and teardown. This type of signaling is considered out-of-band signaling because the Q.931 messages are sent in the D channel only.



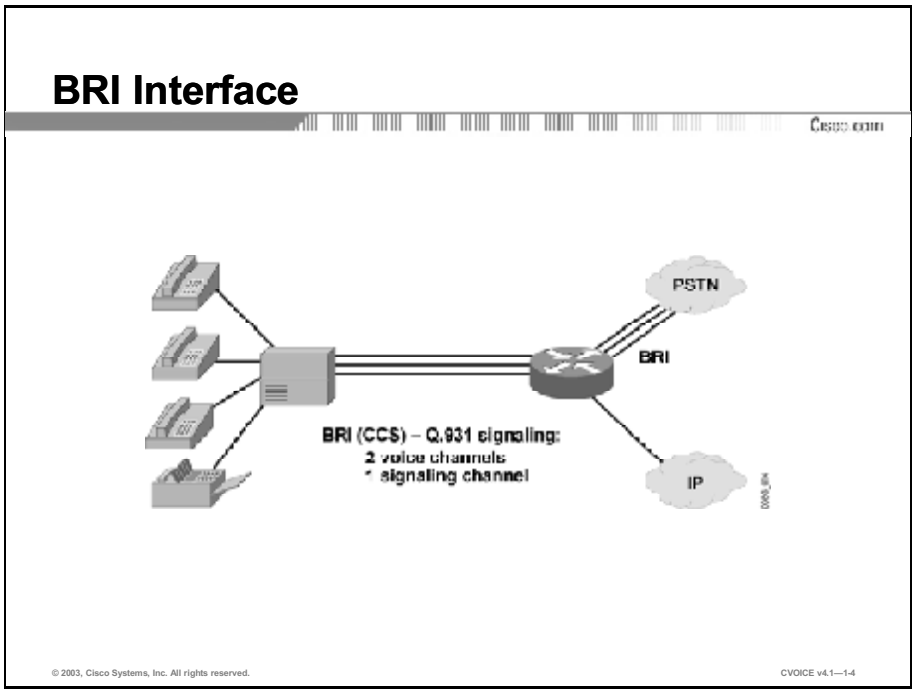
This figure depicts an E1 interface. An E1 interface has 32 channels and simultaneously carries up to 30 conversations. The other two channels are used for framing and signaling. The 32 channels are grouped to form a frame. The frames are then grouped together into multiframes (groups of 16 frames). Europe and Mexico use the E1 interface.

Although you can configure the E1 interface for either CAS or CCS, the most common usage is CCS.

When an E1 interface uses CAS, signaling travels out of band in the signaling channel but follows a strict association between the signal carried in the signaling channel and the channel to which the signaling is being applied. The signaling channel is channel 16.

In the first frame, channel 16 carries 4 bits of signaling for channel 1 and 4 bits of signaling for channel 17. In the second frame, channel 16 carries 4 bits of signaling for channel 2 and 4 bits for channel 18, and so on. This process makes it out-of-band CAS.

When an E1 interface uses CCS, Q.931 signaling is used on a single channel, typically channel 17. When configuring for CCS, configure the interface for PRI signaling. When E1 is configured for CCS, channel 16 carries Q.931 signaling messages only.

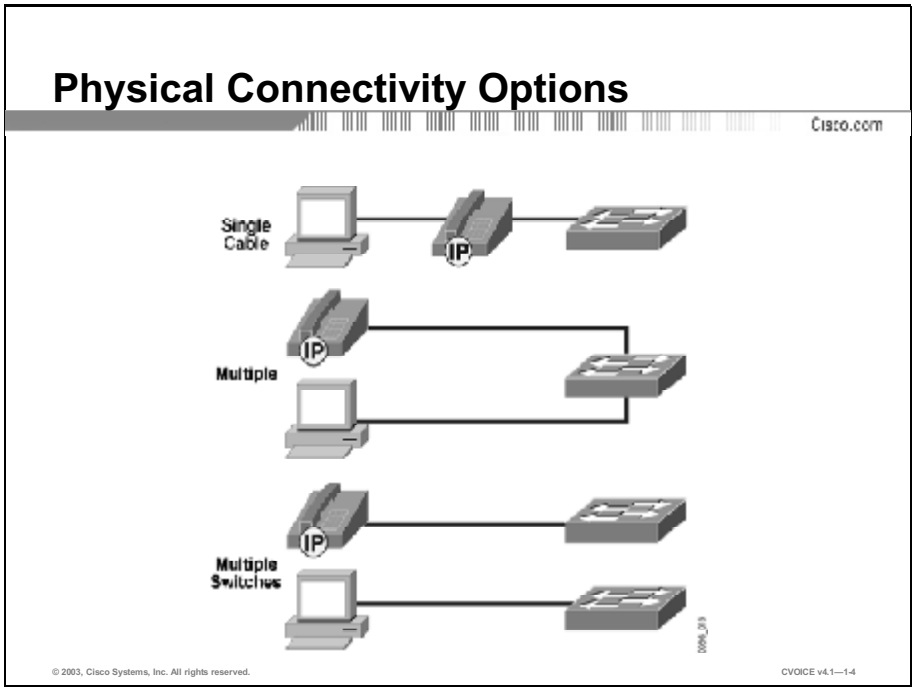


This figure depicts a BRI interface. You can use BRI to connect the PBX voice into the network. Used primarily in Europe for PBX connectivity, BRI provides a 16-kbps D channel for signaling and two 64-kbps B channels for voice. BRI uses Q.931 signaling in the D channel for call signaling.

Note	Cisco Systems does not officially support ISDN telephones.

IP Phones

This topic describes scenarios for desktop telephone connections and the IP Phone built-in switch ports.



This figure depicts physical connection options for IP Phones. The IP Phone connects to the network through an RJ-45 cable. The power-enabled switch port or an external power supply provides power to an IP Phone. The IP Phone functions like other IP-capable devices sending IP packets to the IP network. Because these packets are carrying voice, you must consider both logical and physical configuration issues.

At the physical connection level, there are three options for connecting the IP Phone:

- **Single cable:** A single cable connects the telephone and the PC to the switch. Most enterprises install IP Phones on their networks using a single cable for both the telephone and a PC. Reasons for using a single cable include ease of installation and cost savings on cabling infrastructure and wiring-closet switch ports.

- **Multiple cables:** Separate cables connect the telephone and the PC to the switch. Users often connect the IP Phone and PC using separate cables. This connection creates a physical separation between the voice and data networks.

- **Multiple switches:** Separate cables connect the telephone and the PC to separate switches. With this option, IP Phones are connected to separate switches in the wiring closet. By using this approach you can avoid the cost of upgrading the current data switches and keep the voice and data networks completely separate.

Multiple switches are used in the following situations to:

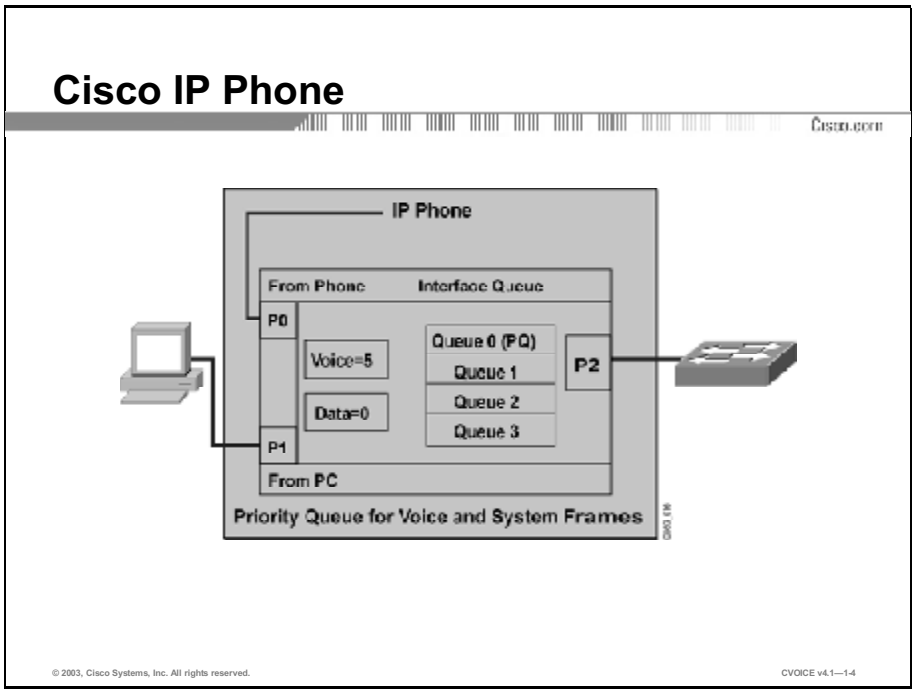
- Provide inline power to IP Phones without having to upgrade the data infrastructure
- Limit the number of switches that need an uninterruptible power supply (UPS)
- Reduce the amount of Cisco IOS® Catalyst software upgrades needed in the network
- Limit the spanning-tree configuration in the wiring-closet switches

The physical configuration for connecting an IP Phone must address the following issues:

- Speed and duplex settings
- Inline power settings

The logical configuration for connecting an IP Phone must address the following issues:

- IP addressing
- VLAN assignment
- Spanning tree
- Classification and queuing



The basic function of a Cisco IP Phone depends on a three-port 10/100 switch. Port P0 is an internal port that connects the voice electronics in the telephone. Port P1 connects a daisy-chained PC. Port P2 uplinks to the Ethernet switch in the wiring closet.

Each port contains four queues with a single threshold. One of these queues is a high-priority queue used for system frames. By default, voice frames are classified for processing in the high-priority queue, and data frames are classified for processing in the low-priority queue.

The internal Ethernet switch on the Cisco IP Phone switches incoming traffic to either the access port or the network port.

If a computer is connected to the access port, data packets traveling to and from the computer, and to and from the phone, share the same physical link to the switch and the same port on the switch. This shared physical link has the following implications for the VLAN network configuration:

- Current VLANs may be configured on an IP subnet basis. However, additional IP addresses may not be available for assigning the phone to the same subnet as the other devices that are connected to the same port.

- Data traffic that is supporting phones on the VLAN may reduce the quality of Voice over IP (VoIP) traffic.

You can resolve these issues by isolating the voice traffic on a separate VLAN for each of the ports connected to a phone. The switch port configured for connecting a phone would have separate VLANs configured to carry the following types of traffic:

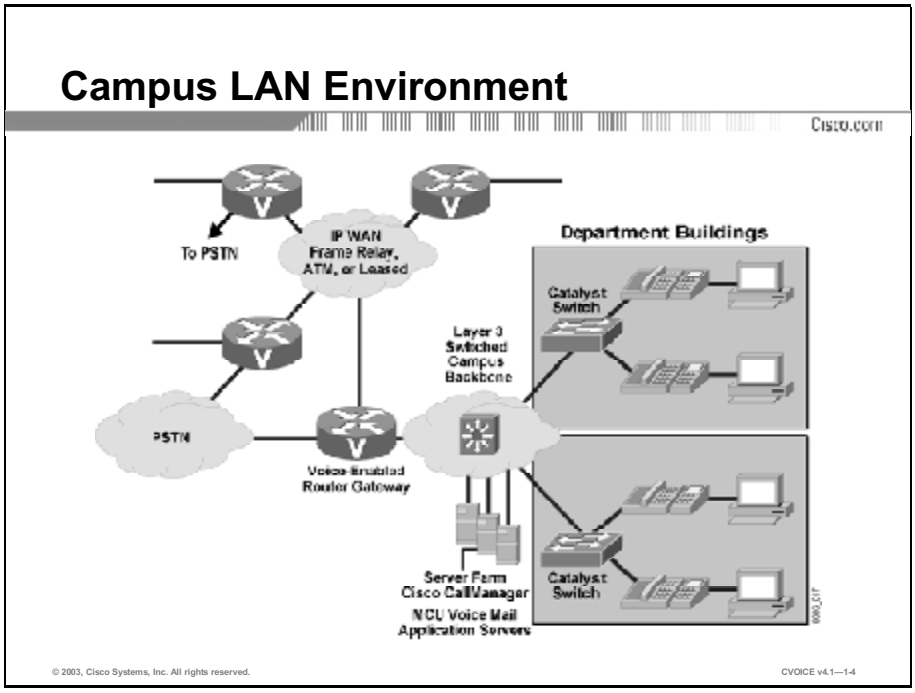
- Voice traffic to and from the IP Phone (auxiliary VLAN)
- Data traffic to and from the PC connected to the switch through the IP Phone access port (native VLAN)

Isolating the phones on a separate auxiliary VLAN increases voice-traffic quality and allows a large number of phones to be added to an existing network that has a shortage of IP addresses.

Note For more information, refer to the documentation included with the Cisco Catalyst switch.

Campus LAN Environment

This topic describes the components used in campus IP telephony installations.



Campus LAN environments have grown tremendously in the past several years due to the demand for networked resources, instant business communication, and voice-over-data applications.

Components for integrated voice and data campus networks include the following:

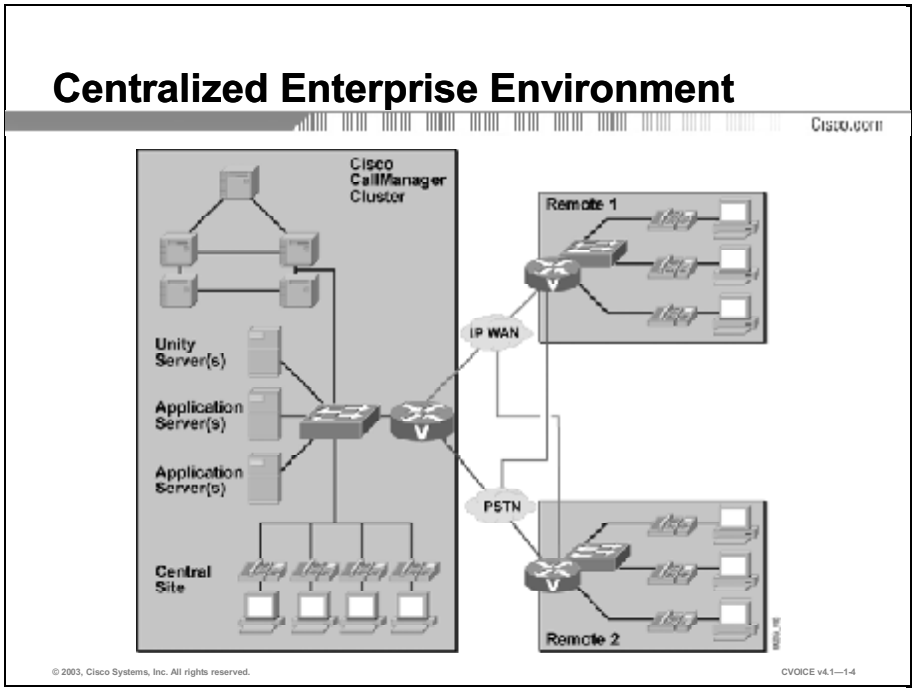
- **IP Phone:** Provides IP voice to the desktop.
- **Cisco CallManager cluster:** Acts as the centralized call-processor for all VoIP devices in the system. The Cisco CallManager cluster is also used for configuring telephones, routing plans for the gateways, and other features. Clustering provides scalability and redundancy.
- **Gateway:** Connects the IP voice to external voice networks, such as the PSTN, or voice devices, such as interactive voice response (IVR) systems or fax machines.
- **Multipoint control unit (MCU):** Provides conferencing capabilities.
- **Application server:** Provides additional services, such as voice mail and unified messaging.

When you are designing the campus infrastructure for voice, you must consider the following key issues:

- Robust, fault-tolerant network design
- Ability to power IP Phones
- Redundant power supply for network components
- Ease of IP addressing
- Quality of service (QoS) enhancements

Enterprise Environment

Enterprise networks grow and evolve as company services and locations change and expand. Heavy reliance on information processing and universal access to corporate information has driven network designs to provide reliable access, redundancy, reachability, and manageability. These same principles apply to designing corporate-wide voice access in the enterprise environment. This topic describes both centralized and distributed enterprise environments.

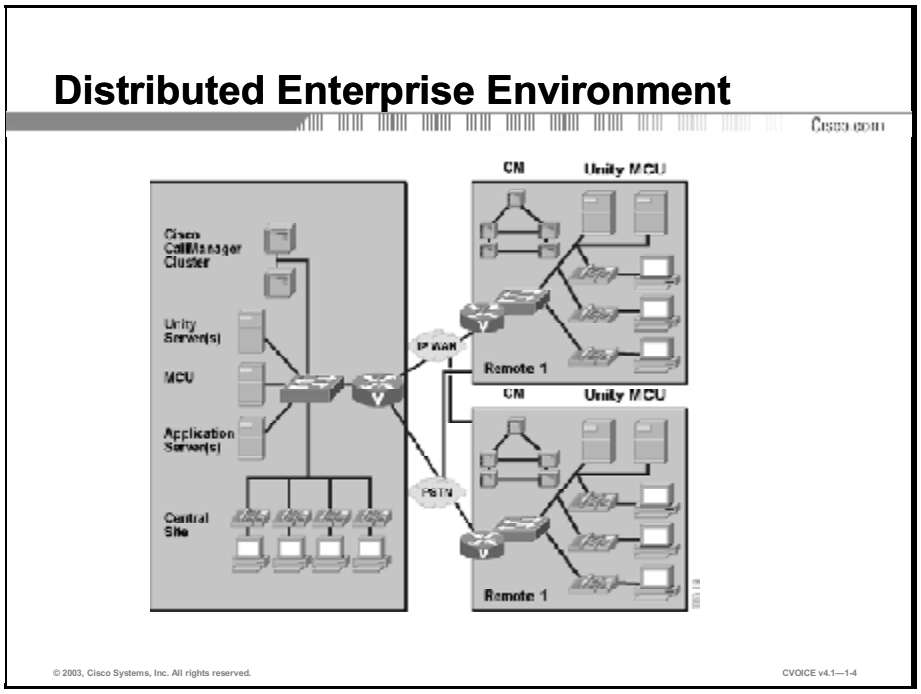


This figure depicts a centralized enterprise environment. Centralized voice networks provide enterprise-wide voice access for calls and voice services controlled from a central site. In this environment, the central site provisions all voice services, such as Cisco CallManager, voice mail, and unified messaging. IP Phones at remote sites connect to Cisco CallManager through the IP WAN for call processing.

Components for centralized voice enterprise networks include:

- **IP Phone:** Provides IP voice to the desktop.
- **Cisco CallManager cluster (central site only):** Acts as the central management console for all VoIP devices in the system and is used for configuring telephones, routing plans for the gateways, and all other features. Clustering provides scalability and redundancy.
- **Gateway (all sites):** Connects the IP voice to external voice networks, such as the PSTN, or to voice devices, such as IVR systems or fax machines.
- **MCU (central site only):** Provides conferencing capabilities.

- **Application server (central site only):** Provides additional services, such as voice mail and unified messaging.
- **Unity server:** Provides a central repository for unified messaging, such as voice-mail, e-mail, and fax.
- **Survivable Remote Site Telephony (SRST) based on Cisco IOS software (remote sites only):** Provides local call-processing capabilities in the event of a WAN outage.
- **IP WAN:** Serves as the primary voice path between sites, with the PSTN as the secondary voice path.



This figure depicts a distributed enterprise environment. Distributed voice networks place voice components at each site and utilize the WAN for intersite calls only.

Components for distributed voice enterprise networks include:

- **IP Phone:** Provides IP voice to the desktop.
- **Cisco CallManager cluster:** Acts as the central management console for all VoIP devices at each site and is used for configuring telephones, routing plans for the gateways, and all other features. Clustering provides scalability and redundancy.
- **Gateway:** Connects the IP voice to external voice networks, such as the PSTN, or voice devices, such as IVR systems or fax machines.
- **MCU:** Provides real-time videoconferencing capabilities.
- **Application server:** Provides additional services, such as voice mail and unified messaging.
- **IP WAN:** Serves as the primary voice path between sites, with the PSTN as the secondary voice path.

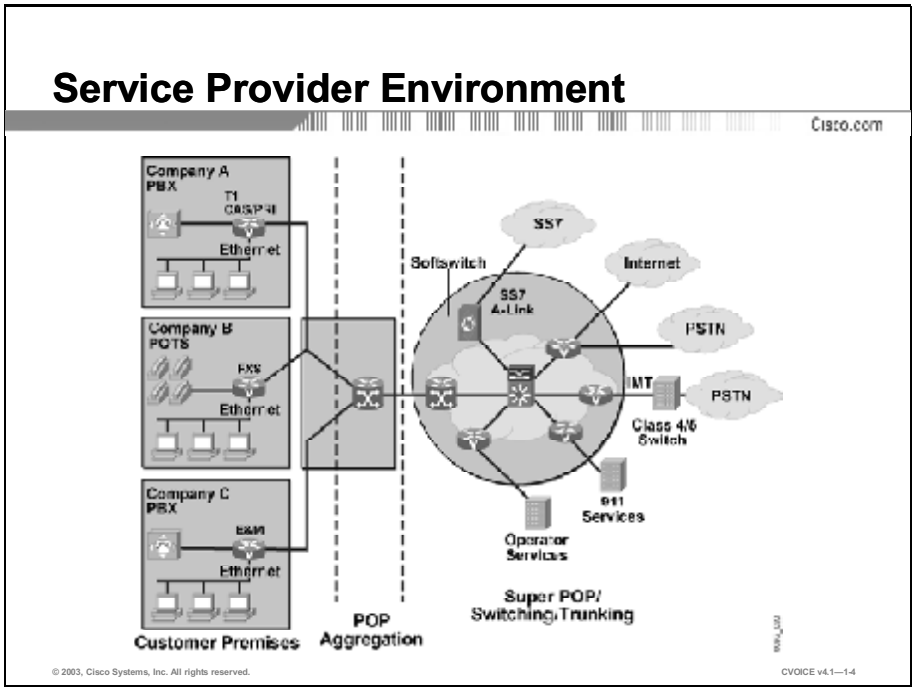
Modern enterprise network applications include:

- E-business
- E-learning

- Customer care
- Unified messaging
- Videoconferencing
- Voice calls placed from web pages

Service Provider Environment

Service provider requirements add another level of complexity to the voice environment. This topic describes basic service provider requirements.



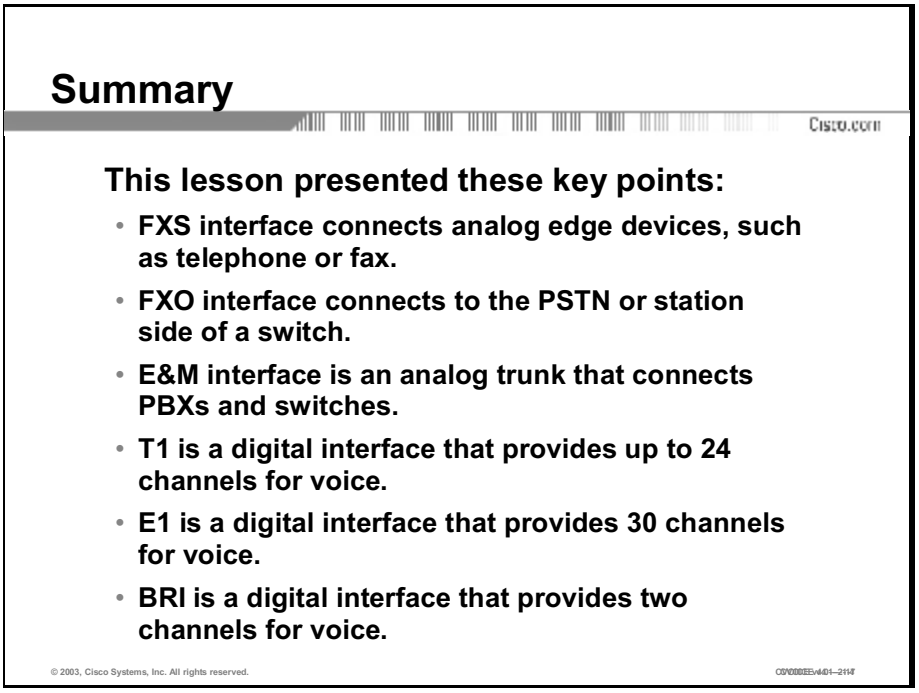
This figure depicts a service provider environment. To be competitive, service providers must provide their business customers with more efficient, less expensive alternatives to the PSTN for voice and data services.

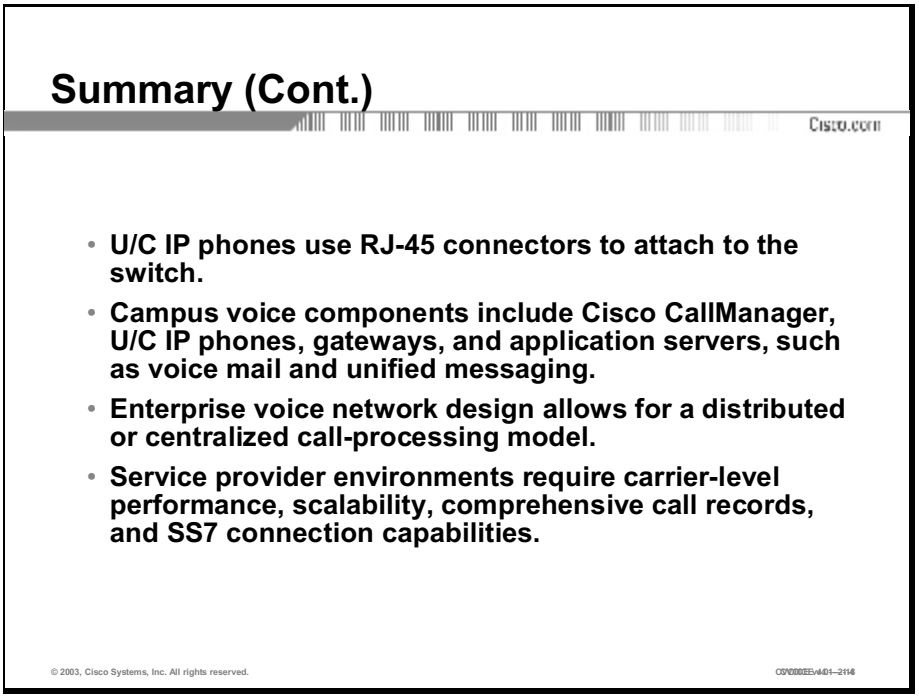
Requirements in the service provider arena include:

- **Carrier class performance:** Voice gateways must provide service that minimizes latency and controls jitter. This level of performance allows customers to maintain voice quality as they migrate from circuit-switched voice to IP-based services.
- **Scalability:** Design must accommodate rapid growth to enable service providers to grow with their customer base. An important aspect of scalability is the automation, configuration, and administration of IP networks and gateways for seamless expansion.
- **Comprehensive call records supporting flexible service pricing:** This is the ability to extract IP session and transaction information from multiple network devices and from all layers of the network—in real time—to produce detailed billing records.
- **Signaling System 7 interconnect capabilities:** Tariffs favor interconnection using Signaling System 7 (SS7) signaling, because Inter-Machine Trunks (IMTs) are less expensive than ISDN-based facilities. This financial benefit equates to lower monthly expenses, the reduced cost of goods that are sold, and higher margins for service providers.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): IP Telephony Applications
- Analog and Digital Voice Connections module

References

For additional information, refer to these resources:

- "Multisite WAN with Distributed Call Processing"
  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network/dgdistrb.htm
- "Multisite WAN with Centralized Call Processing"
  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network/dgcentrl.htm
- "Connecting IP Phones"
  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/avvidqos/qosphone.htm

Quiz: IP Telephony Applications

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the three basic analog interfaces and the telephony devices that they connect
- Describe the three basic digital interfaces and the type of signaling that each interface supports
- Describe the three physical connectivity options for IP Phones and explain the functioning of the Cisco IP Phone
- List five basic components of an integrated voice and data campus LAN network
- Explain the difference between distributed and centralized enterprise environments and list five main components of each type of enterprise network
- List four capabilities that allow service provider networks to offer more efficient, less expensive alternatives to the Public Switched Telephone Network

Instructions

Answer these questions.

Q1) In E&M signaling, “E” refers to the _____.

A) electromagnet

B) ring

C) electrical ground

D) tip

E) Erlang

Q2) The FXS interface provides a direct connection to the _____.

A) CO

B) E&M trunk

C) telephone

D) gatekeeper

Q3) An E1 interface can carry up to _____ conversations simultaneously.

A) 16

B) 24

C) 30

D) 32

Q4) What type of signaling is used when a T1 interface uses CCS?

A) robbed-bit signaling

B) Megaco

C) Q.931

D) H.323

Q5) What kind of cable is used to connect an IP Phone to the network?

A) RJ-11

B) wireless transceiver

C) serial crossover

D) RJ-41

E) RJ-45

Q6) How many queues does each port on a Cisco IP Phone contain?

A) 2

B) 3

C) 4

D) 12

Q7) In a campus LAN environment, the multipoint control unit provides _____.

A) central call-processing capabilities

B) configuration capabilities

C) conferencing capabilities

D) extended-calling capabilities

E) call-pickup capabilities

Q8) Which two of the following key issues must be considered when designing the campus infrastructure for voice? (Choose two.)

A) ability to power IP Phones

B) processing power of the gatekeeper

C) size of DRAM in the routers

D) ease of IP addressing

Q9) Which two models are used for designing enterprise networks? (Choose two.)

A) service provider

B) carrier class

C) distributed

D) centralized

E) remote site

Q10) What is the function of the SRTS component of a centralized voice enterprise network?

A) connects IP Phones on remote sites to Cisco CallManager

B) provides local call-processing capabilities in case of a WAN outage

C) configures routing plans for the gateways

D) serves as the primary voice path between sites

Q11) To be competitive, service providers must provide their business customers with _____ alternatives to the PSTN for voice and data services.

A) more extensive, less complicated

B) more exhaustive, less limited

C) more digital, less analog

D) more efficient, less expensive

Q12) In service provider environments, the network design must accommodate _____.

A) support for TDM

B) automated configuration of IP networks

C) support for SIP, H.323, and MGCP

D) a full Class A IP-address block

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

2

Analog and Digital Voice Connections

Overview

Cisco voice devices must support a wide variety of connection types. This module describes the various analog and digital connections, introduces quality issues, describes common compression schemes, and concludes with a description of fax over IP voice networks.

Upon completing this module, you will be able to:

- Select the appropriate analog voice connection to a Cisco device given the types of analog connections and their susceptibility to line quality problems
- Choose a voice compression scheme that best suits your needs given the fundamentals of digital voice encoding
- Describe the appropriate signaling method to deploy in a telephony system given the type of signaling: between PBXs; between PBXs and central offices; or specialized, such as ISDN
- Implement an effective method of transporting fax and modem traffic over a Voice over IP network given the standard implementations of fax and the methods used to transport modem traffic

Outline

The module contains these lessons:

- Analog Voice Basics
- Analog to Digital Voice Encoding
- Signaling Systems
- Fax and Modem over VoIP

Analog Voice Basics

Overview

Interfacing Cisco Systems equipment with traditional analog telephony devices requires an understanding of the various interfaces used in the industry. This lesson explains the types of analog connections that are used and their susceptibility to line quality problems.

Importance

To correctly choose and implement an analog voice connection to a Cisco device, you must understand the types of interfaces that are used in the industry and their line quality effects.

Objectives

Upon completing this lesson, you will be able to:

- Identify the components of local-loop connections
- Identify the signaling used on local loops
- Identify on-hook, off-hook, and ringing-supervisory signaling
- Identify pulse dialing and dual tone multifrequency
- List the call-progress indicators and their functions
- State the purpose and types of trunk connections
- Identify the signaling used on trunks
- Identify the five types of wiring schemes used in ear and mouth signaling
- Describe Wink-Start, immediate-start, and delay-start signaling

- Describe impairments that interfere with line quality
- Identify two methods that are used in the industry to reduce the problem of echo

Learner Skills and Knowledge

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

- Familiarity with telephony station equipment, such as handsets and fax machines
- Familiarity with telephony switching equipment, such as key systems and PBXs

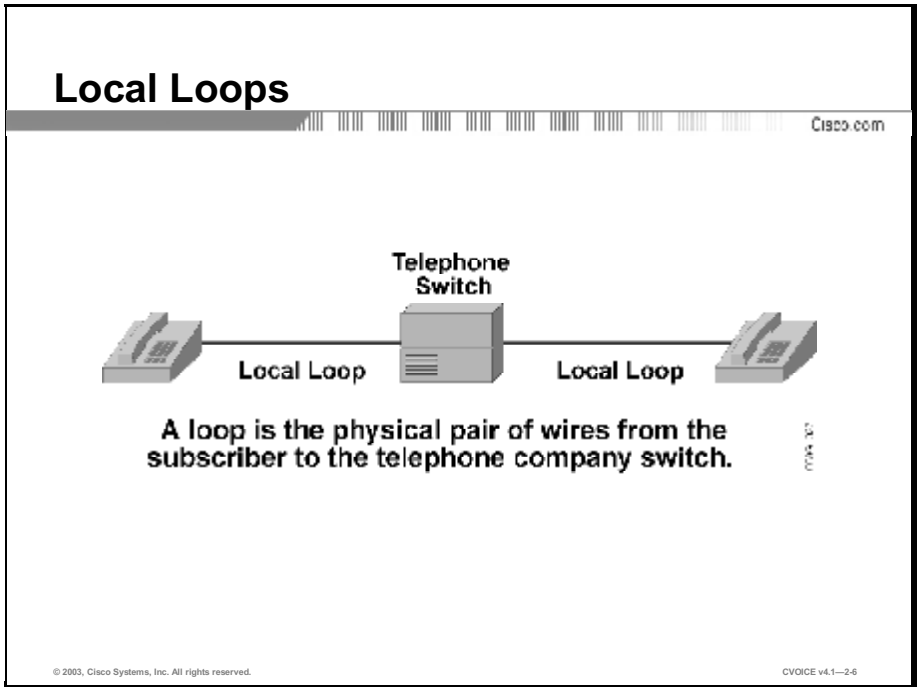
Outline

This lesson includes these topics:

- Overview
- Local-Loop Connections
- Types of Local-Loop Signaling
- Supervisory Signaling
- Address Signaling
- Informational Signaling
- Trunk Connections
- Types of Trunk Signaling
- Ear and Mouth Signaling Types
- Trunk Signal Types Used by Ear and Mouth
- Line Quality
- Management of Echo
- Summary
- Assessment (Quiz): Analog Voice Basics
- Assessment (Complex Lab): Lab Exercise 2-1

Local-Loop Connections

This topic describes the parts of a traditional telephony local-loop connection between a telephone subscriber and the telephone company.

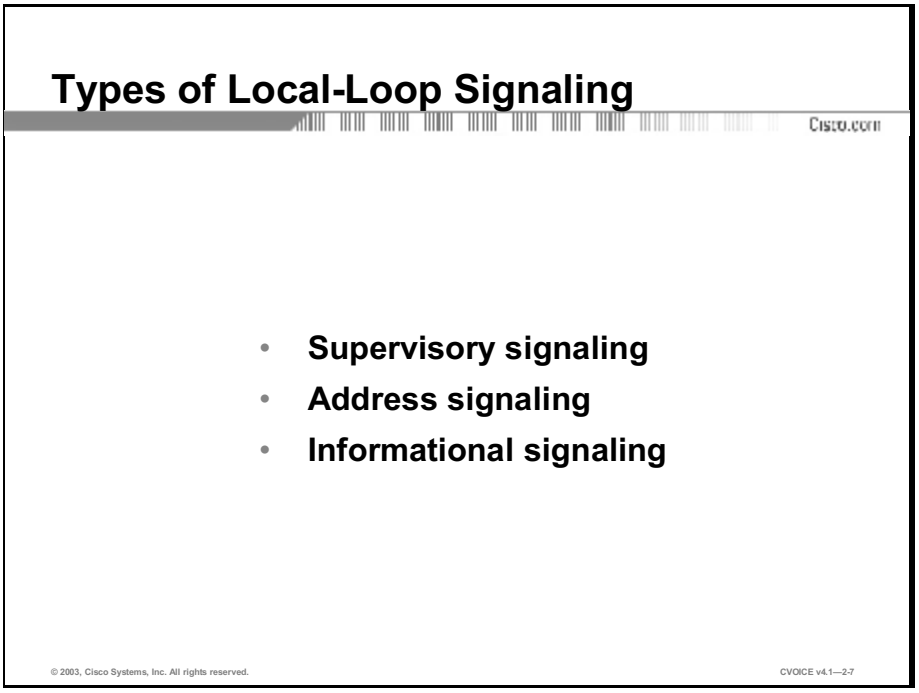


A subscriber home telephone connects to the telephone company central office (CO) via an electrical communication path called a local loop, as depicted in the figure. The loop consists of a pair of twisted wires—one is called *tip,* the other is called *ring*.

In most arrangements, the ring wire ties to the negative side of a power source, called *battery*, while the tip wire connects to the ground. When you take your telephone off hook, current flows around the loop, allowing dial tone to reach your handset. Your local loop, along with all the others in your neighborhood, connects to the CO in a cable bundle, either buried underground or strung on poles.

Types of Local-Loop Signaling

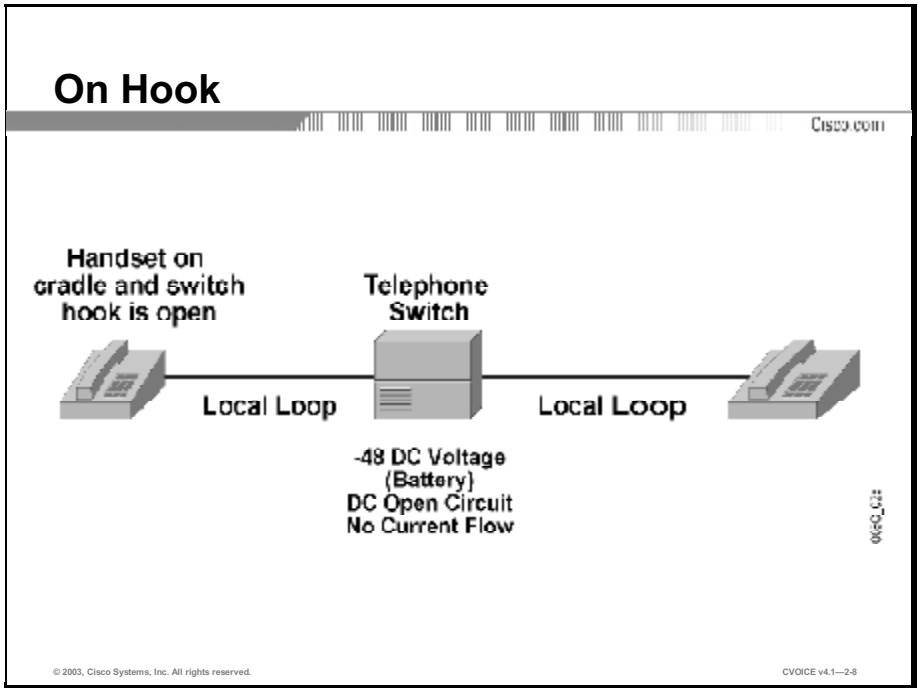
This topic explains local-loop signaling and lists some of the signaling types.



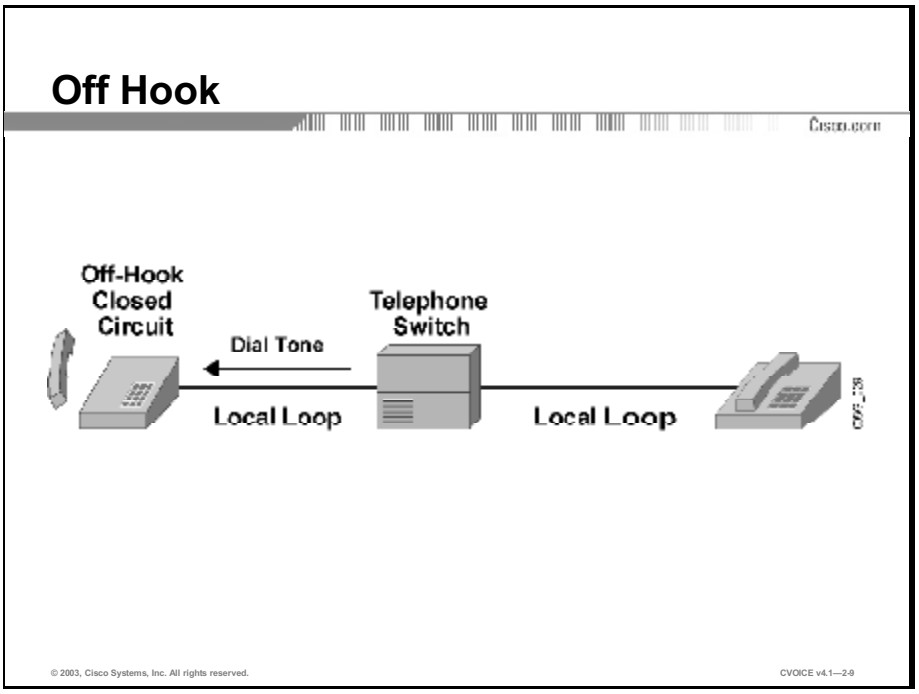
A subscriber and telephone company notify each other of the call status through audible tones and an exchange of electrical current. This exchange of information is called local-loop signaling.

Supervisory Signaling

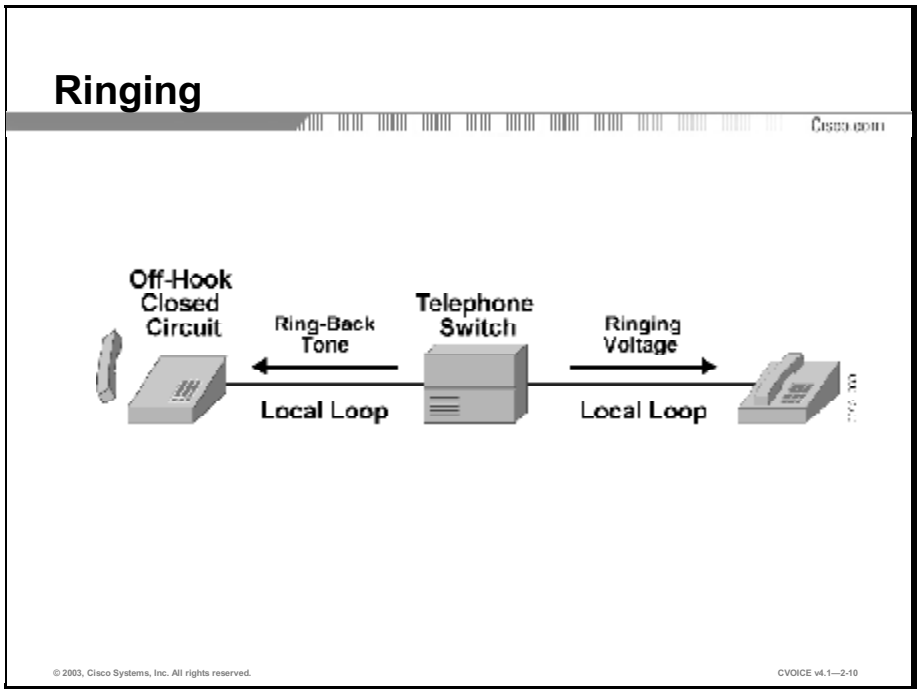
This topic describes on-hook, off-hook, and ringing-supervisory signaling.



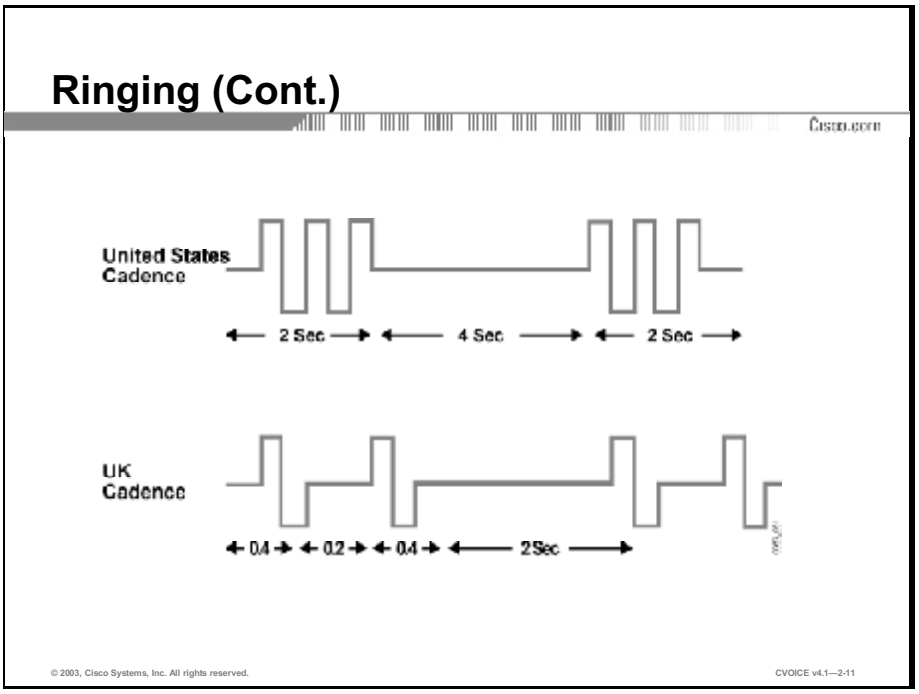
Resting the handset on the telephone cradle opens the switch hook and prevents the circuit current from flowing through the telephone. Regardless of the signaling type, a circuit goes on hook when the handset is placed on the telephone cradle and the switch hook is toggled to an open state. When the telephone is in this position, only the ringer is active.



When a subscriber wants to place a call, that subscriber must lift the handset from the telephone cradle. Removing the handset from the cradle places the circuit off hook. The switch hook is then toggled to a closed state, causing circuit current to flow through the electrical loop. The current notifies the telephone company that someone is requesting to place a telephone call. When the telephone network senses the off-hook connection by the flow of current, it provides a signal in the form of the dial tone to indicate that it is ready.



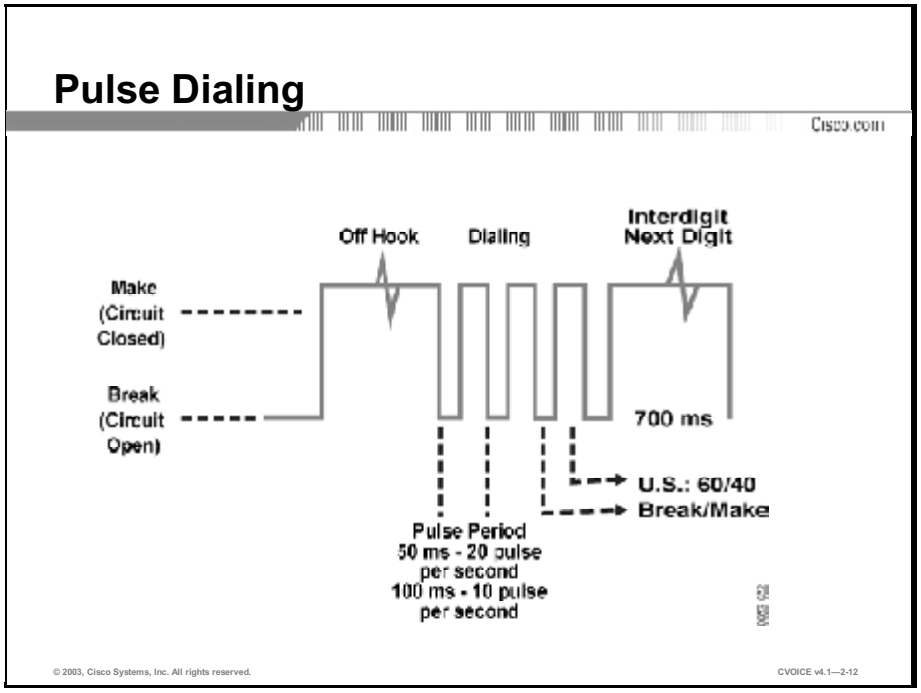
When a subscriber makes a call, the telephone sends voltage to the ringer to notify the other subscriber of an inbound call. The telephone company also sends a ringback tone to the caller, alerting the caller that it is sending ringing voltage to the recipient telephone. Although ringback tone is not the same as ringing voltage, it sounds similar.



As depicted in the figure, the ringing supervision tone in the United States is 2 seconds of tone followed by 4 seconds of silence. Europe uses a double ring of 0.4 seconds separated by 0.2 seconds of silence, followed by 2 seconds of silence.

Address Signaling

This topic describes pulse dialing and dual-tone multifrequency (DTMF) signaling.

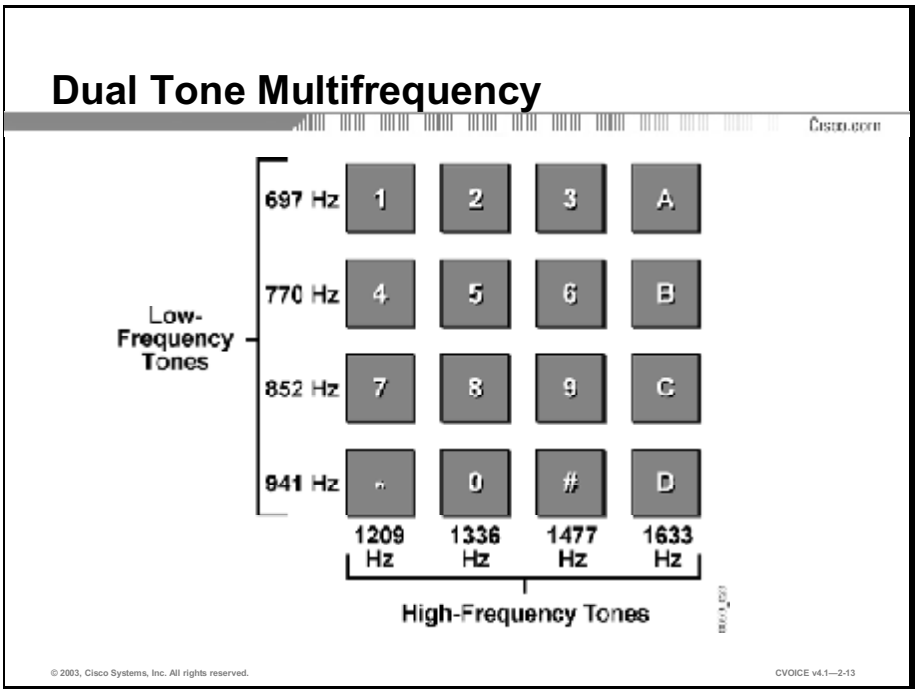


Although somewhat outdated, rotary-dial telephones are still in use and easily recognized by their large numeric dial-wheel. When placing a call, the subscriber spins the large numeric dial-wheel to send digits. These digits must be produced at a specific rate and within a certain level of tolerance. Each pulse consists of a “break” and a “make.” The break segment is the time that the circuit is open. The make segment is the time during which the circuit is closed. In the United States, the break/make cycle must correspond to a ratio of 60-percent break to 40-percent make.

A “governor” inside the dial controls the rate at which the digits are pulsed.

The dial pulse signaling process occurs as follows:

1. When a subscriber calls someone by dialing a digit on the rotary dial, a spring winds.
2. When the dial is released, the spring rotates the dial back to its original position.
3. While the spring rotates the dial back to its original position, a cam-driven switch opens and closes the connection to the telephone company. The number of consecutive opens and closes—or breaks and makes—represents the dialed digit.

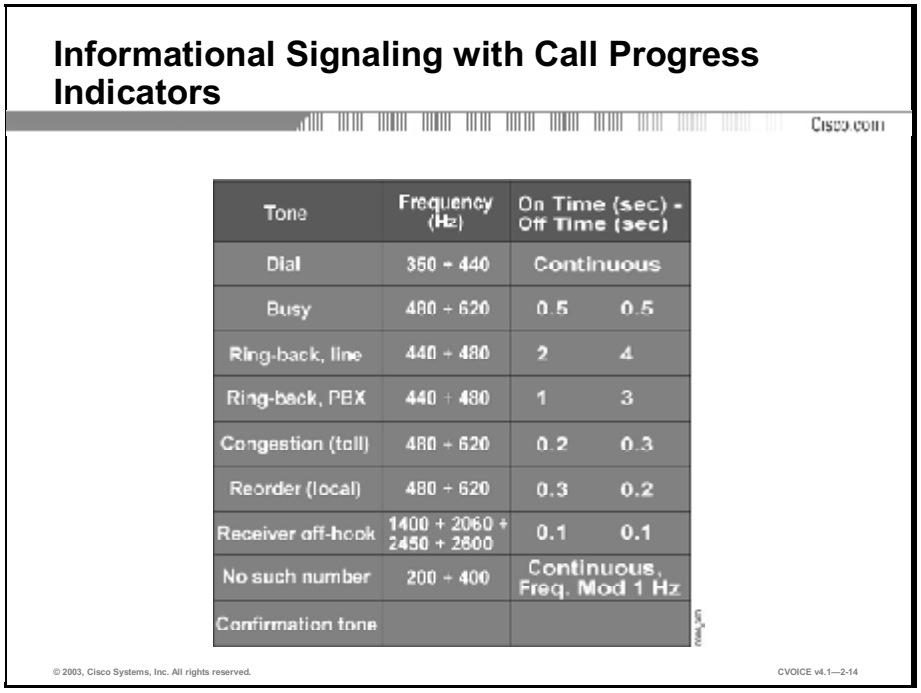


Users who have a touch-tone pad or a push-button telephone must push the keypad buttons to place a call. Each button on the keypad is associated with a set of high and low frequencies. Each row of keys on the keypad is identified by a low-frequency tone; each column of keys on the keypad is identified by a high-frequency tone. The combination of both tones notifies the telephone company of the number being called, hence the term *dual tone multifrequency* (DTMF).

The figure illustrates the combination of tones generated for each button on the keypad.

Informational Signaling

This topic lists the call-progress indicators and describes their functions.



Call-progress indicators in the form of tone combinations are used to notify subscribers of call status. Each combination of tones represents a different event in the call process. These different events include:

- **Dial tone:** Indicates that the telephone company is ready to receive digits from the user telephone. The Cisco routers provide dial tone as a method of showing that the hardware is installed. In a PBX or key telephone system, the dial tone indicates that the system is ready to receive digits.

- **Busy:** Indicates that a call cannot be completed because the telephone at the remote end is already in use.

- **Ringback (normal or PBX):** Indicates that the telephone company is attempting to complete a call on behalf of a subscriber.

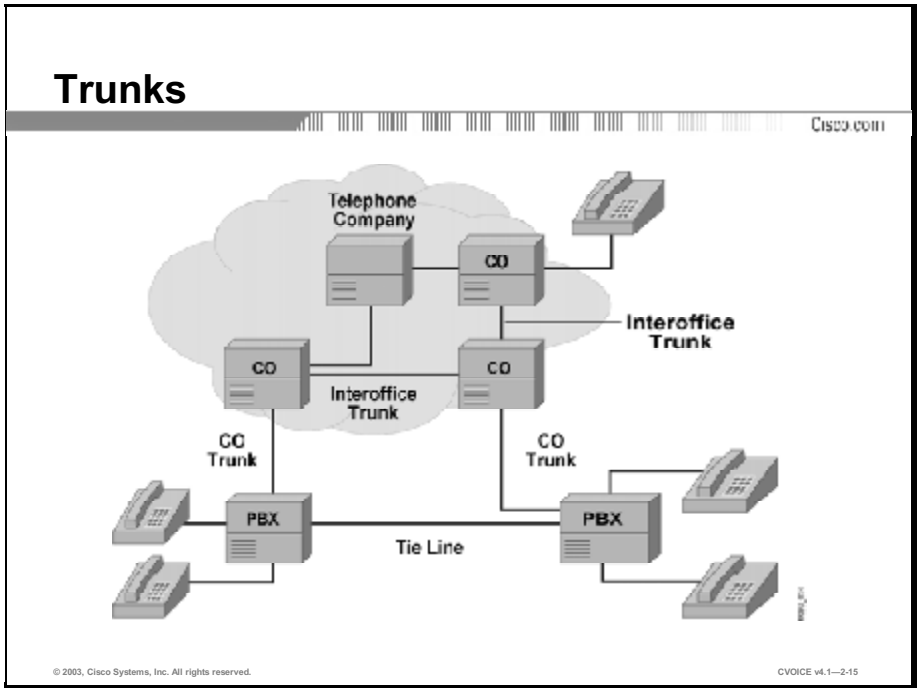
- **Congestion:** Indicates that congestion in the long-distance telephone network is preventing a telephone call from being processed. The congestion tone is sometimes known as the all-circuits-busy tone.

- **Reorder tone:** Indicates that all of the local telephone circuits are busy, thus preventing a telephone call from being processed. The reorder tone is known to the user as fast-busy, and is familiar to anyone who operates a telephone from a PBX.

- **Receiver off hook:** Indicates that the receiver has been off hook for an extended period without placing a call.
- **No such number:** Indicates that a subscriber placed a call to a nonexistent number.
- **Confirmation tone:** Indicates that the telephone company is working on completing the call.

Trunk Connections

This topic describes the different types of trunks on a voice network and how they operate.



Before a telephone call terminates at its final destination, it is routed through multiple switches. When a switch receives a call, it determines whether the destination telephone number is within a local switch or if the call needs to go through another switch to a remote destination. Trunks connect the telephone company and PBX switches.

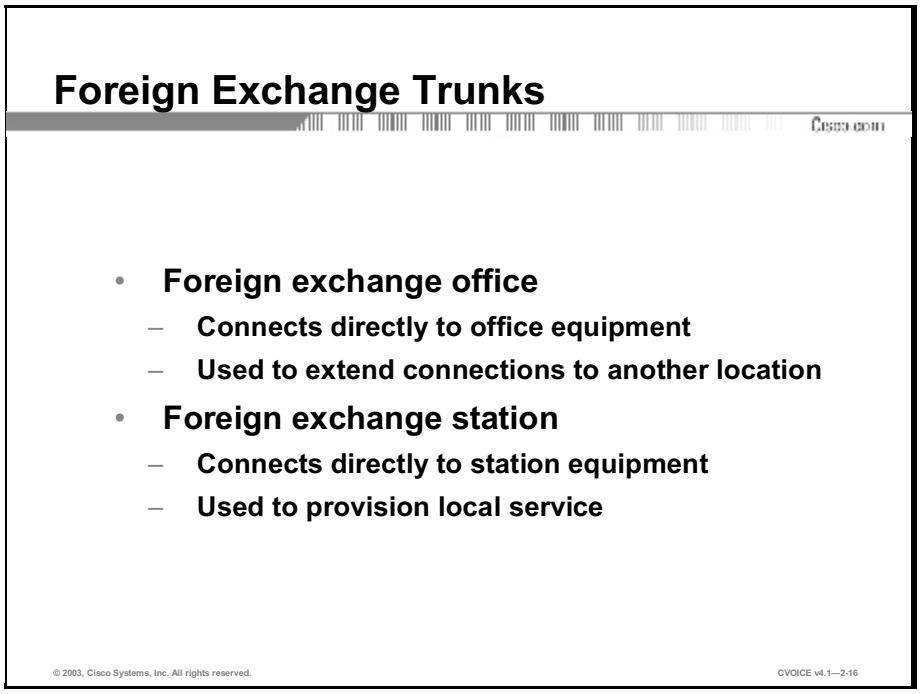
The primary function of the trunk is to provide the path between switches. The switch must route the call to the correct trunk or telephone line. Although many different subscribers share a trunk, only one subscriber uses it at any given time. As telephone calls end, they release trunks and make them available to the switch for subsequent calls. There can be several trunks between two switches.

The following are examples of the more common trunk types:

- **Private trunk lines:** Companies with multiple PBXs often connect them with tie trunk lines. Generally, tie trunk lines serve as dedicated circuits that connect PBXs. On a monthly basis, subscribers lease trunks from the telephone company to avoid the expense of using telephone lines on a per-call basis. These types of connections, known as tie-lines, typically use special interfaces called recEive and transMit, or ear and mouth (E&M), interfaces.

- **CO trunks:** A CO trunk is a direct connection between a PBX and the local CO that routes calls; for example, the connection from a private office network to the Public Switched Telephone Network (PSTN). When users dial **9**, they are connecting through their PBX to the CO trunk to access the PSTN. CO trunks typically use Foreign Exchange Office (FXO) interfaces. Certain specialized CO trunks are frequently used on the telephony network. A direct inward dial (DID) trunk, for example, allows outside callers to reach specific internal destinations without having to be connected via an operator.

- **Interoffice trunks:** An interoffice trunk is a circuit that connects two local telephone company COs.



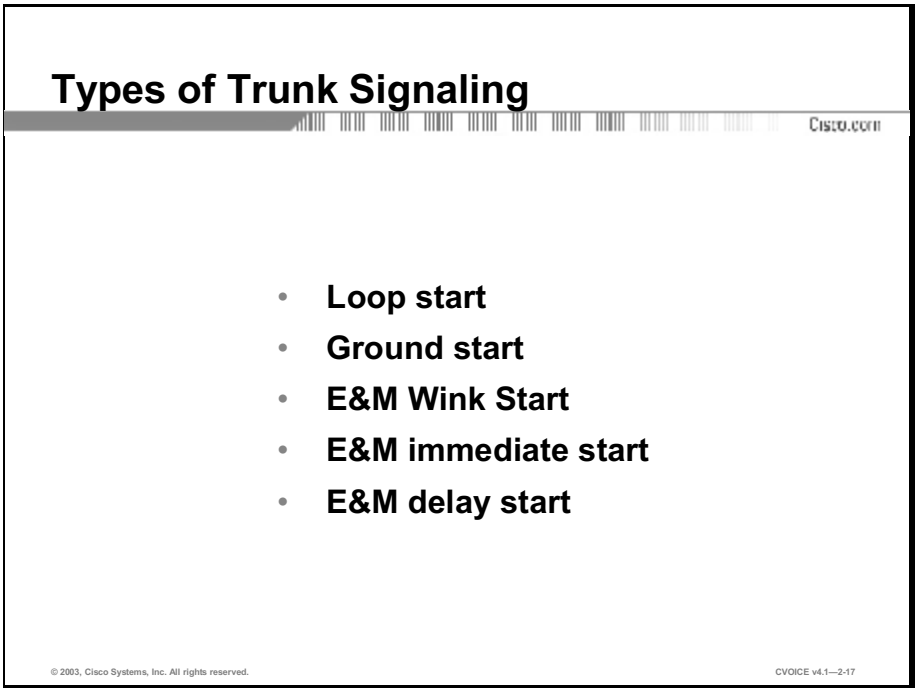
- **Foreign exchange (FX) trunks:** FX trunks are interfaces that are connected to switches that support connection to either station equipment or office equipment. Station equipment includes telephones, fax machines, and modems. Office equipment includes other switches (to extend the connection) and Cisco devices.

- **FXO interfaces:** An FXO interface connects the PBX to another switch or Cisco device. The purpose of an FXO interface is to extend the telephony connection to a remote site; for example, if a user on a corporate PBX wanted a telephone installed at home instead of in the local office where the PBX is located, an FXO interface would be used. The FXO interface would connect to a Cisco voice router, which would serve to extend the connection to the user home. This connection is an Off-Premises eXtension (OPX).

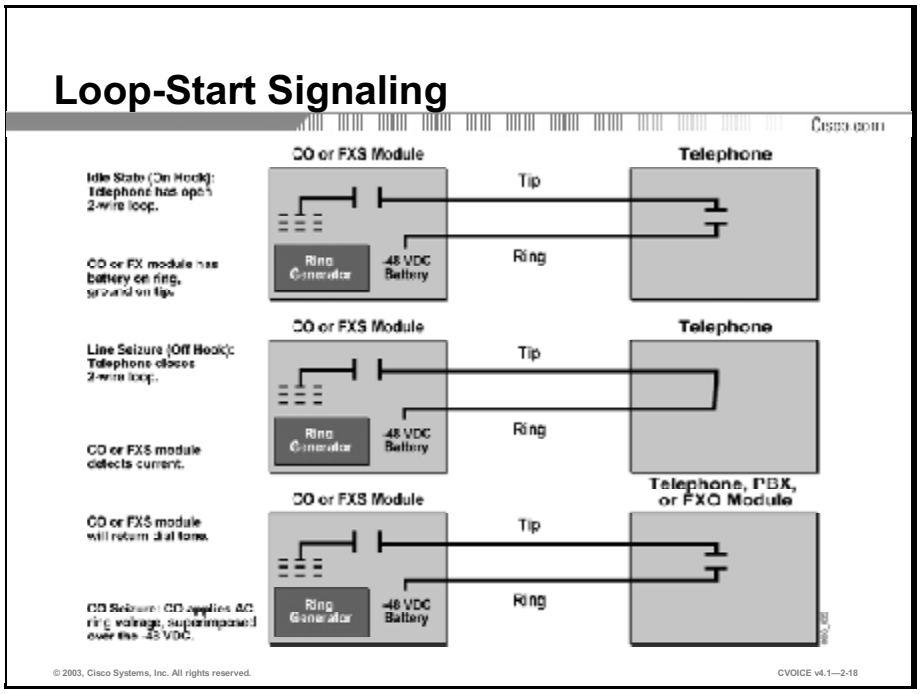
- **Foreign Exchange Station (FXS) interfaces:** An FXS interface connects station equipment. A telephone connected directly to a switch or Cisco device requires an FXS interface. Because a home telephone connects directly to the telephone company CO switch, an FXS interface is used.

Types of Trunk Signaling

This topic describes the trunk and/or line-seizure signaling types.



There must be signaling standards between the lines and trunks of a telephone network, just as there are signaling standards between a telephone and the telephone company.



Loop-start signaling allows a user or the telephone company to seize a line or trunk when a subscriber is initiating a call. It is primarily used on local loops rather than on trunks.

A telephone connection exists in one of the following states:

- Idle (on hook)
- Telephone seizure (off hook)
- CO seizure (ringing)

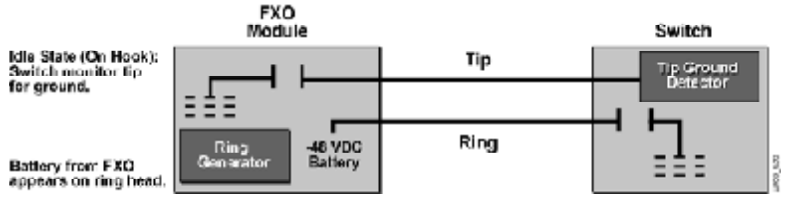
A summary of the loop-start signaling process is as follows:

1. When the line is in the idle state, or on hook, the telephone or PBX opens the two-wire loop. The CO or FXS has *battery* on ring and *ground* on tip.
2. If a user lifts the handset off the cradle to place a call, the switch hook goes off hook and closes the loop (line seizure). The current can now flow through the telephone circuit. The CO or FXS module detects the current and returns a dial tone.
3. When the CO or FXS module detects an incoming call, it applies AC ring voltage superimposed over the –48 VDC battery, causing the ring generator to notify the recipient of a telephone call. When the telephone or PBX answers the call, thus closing the loop, the CO or FXS module removes the ring voltage.

Loop-start signaling is a poor solution for high-volume trunks because it leads to glare incidents or the simultaneously seizure of the trunk from both ends. Glare occurs, for example, when you pick up your home telephone and find that someone is already at the other end.

Glare is not a significant problem at home. It is, however, a major problem when it occurs between switches at high-volume switching centers, such as long-distance carriers.

Ground-Start Signaling

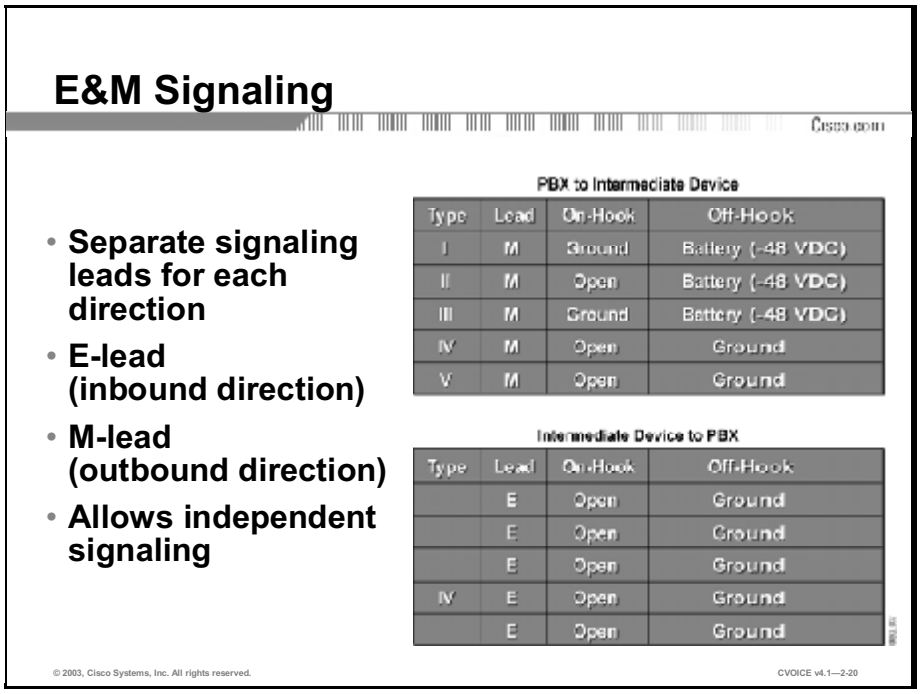


Ground-start signaling is a modification of loop-start signaling that corrects for the probability of glare. It solves the problem by providing current detection at both ends.

Although loop-start signaling works when you use your telephone at home, ground-start signaling is preferable when there are high-volume trunks involved at telephone switching centers. Because ground-start signaling uses a request and/or confirm switch at both ends of the interface, it is preferable over other signaling methods on high-usage trunks, such as FXOs.

FXOs require implementation of answer supervision (reversal or absence of current) on the interface for the confirmation of on hook and/or off hook.

Ground-start signaling is not common in Voice over IP (VoIP) networks.



E&M signaling supports tie-line type facilities or signals between voice switches. Instead of superimposing both voice and signaling on the same wire, E&M uses separate paths, or *leads,* for each.

Example

To call a remote office, your PBX must route a request for use of the trunk over its signal leads between the two sites. Your PBX makes the request by activating its M-lead. The other PBX detects the request when it detects current flowing on its E-lead. It then attaches a dial register to the trunk and your PBX, which sends the dialed digits. The remote PBX activates its M-lead to notify you that the call is complete.

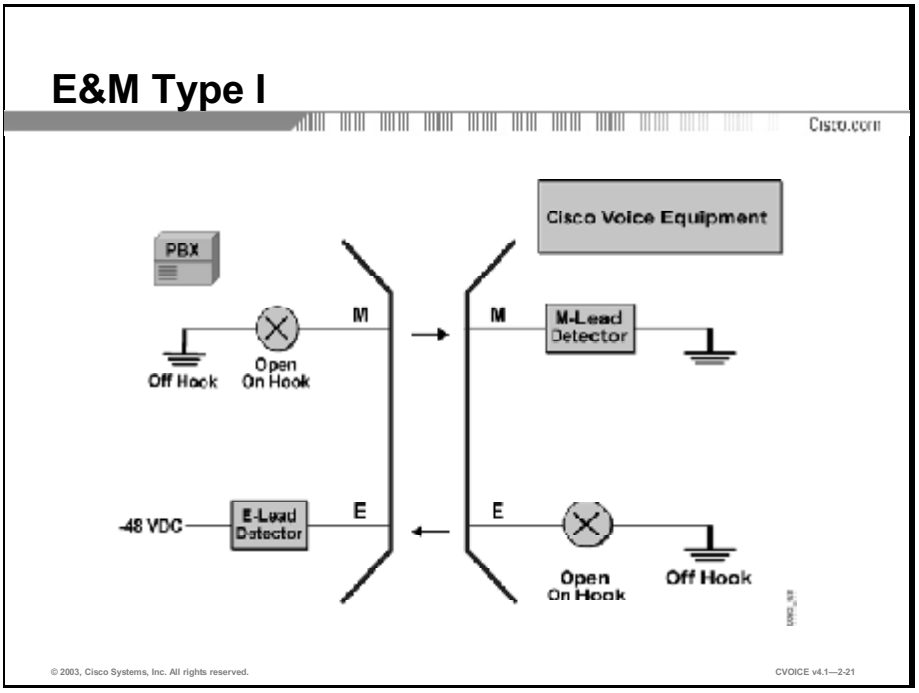
Types of E&M Signaling

There are five types of E&M signaling: Type I, Type II, Type III, Type IV, and Type V. The E&M leads operate differently with each wiring scheme, as shown in the table here.

E&M Signaling Type	PBX to Intermediate Device			Intermediate Device to PBX		
	Lead	On Hook	Off Hook	Lead	On Hook	Off Hook
Type I	M	Ground	Battery (–48 VDC)	E	Open	Ground
Type II	M	Open	Battery (–48 VDC)	E	Open	Ground
Type III	M	Ground	Battery (–48 VDC)	E	Open	Ground
Type IV	M	Open	Ground	E	Open	Ground
Type V	M	Open	Ground	E	Open	Ground

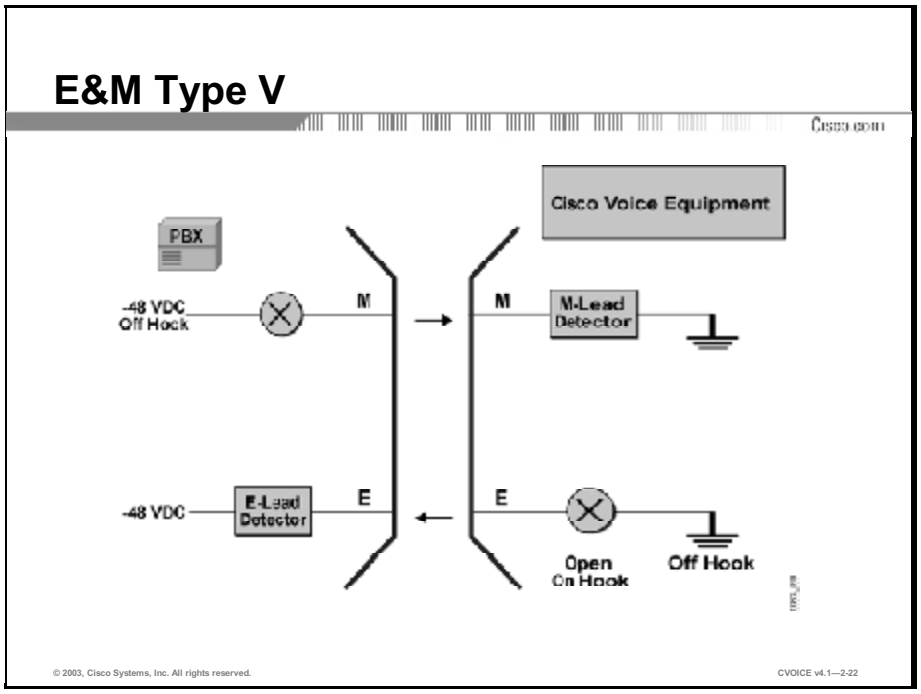
Ear and Mouth Signaling Types

This topic identifies the five E&M signaling types and provides a description of each.



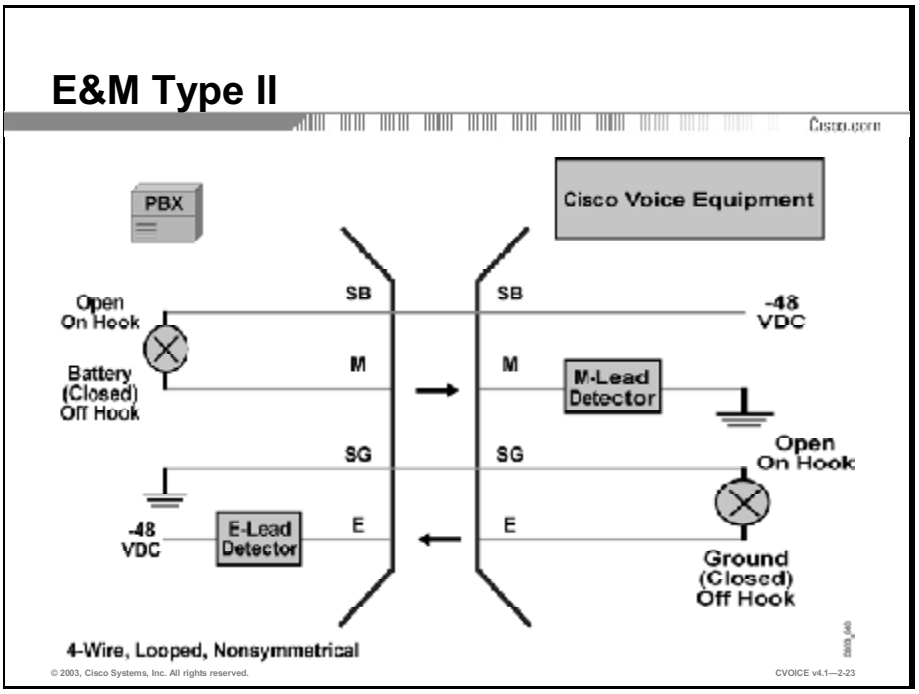
Four-wire E&M Type I signaling is actually a six-wire E&M signaling interface common in North America. One wire is the E-lead; the second wire is the M-lead, and the remaining two pairs of wires serve as the audio path. In this arrangement, the PBX supplies power, or *battery*, for both the M- and E-leads, shown in the figure. This arrangement also requires that a common ground be connected between the PBX and the Cisco voice equipment.

With the Type I interface, the Cisco voice equipment (tie-line equipment) generates the E signal to the PBX by grounding the E-lead. The PBX detects the E signal by sensing the increase in current through a resistive load. Similarly, the PBX generates the M signal by sourcing a current to the Cisco voice equipment (tie-line equipment), which detects it via a resistive load.



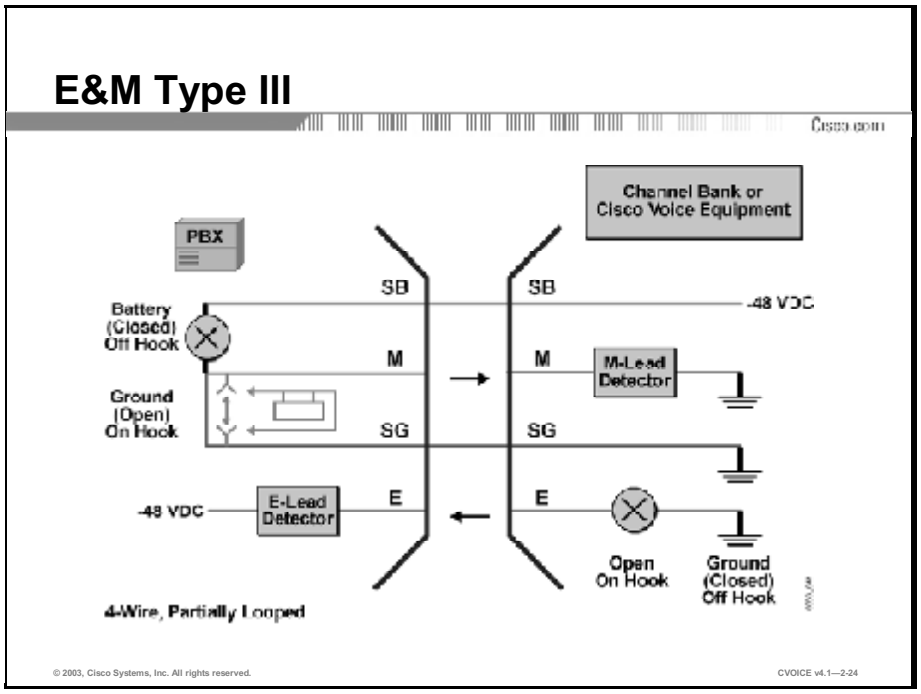
Type V is another six-wire E&M signaling type and the most common E&M signaling form outside of North America. In Type V, one wire is the E-lead and the other wire is the M-lead.

Type V is a modified version of the Type I interface. In the Type V interface, the Cisco voice equipment (tie-line equipment) supplies battery for the M-lead while the PBX supplies battery for the E-lead. As in Type I, Type V requires that a common ground be connected between the PBX and the Cisco voice equipment.

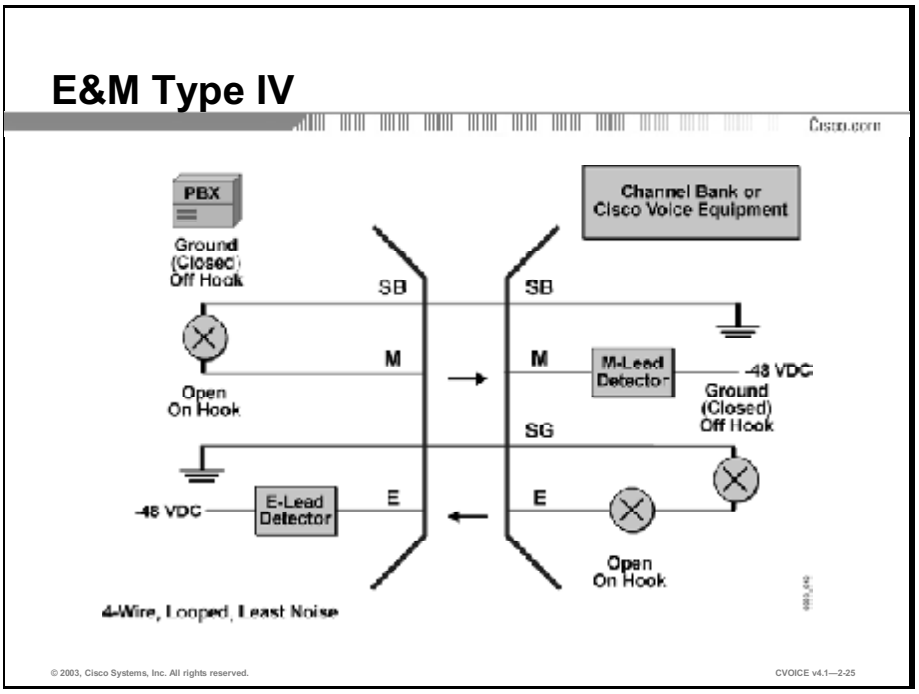


Types II, III, and IV are eight-wire interfaces. One wire is the E-lead, the other wire is the M-lead. Two other wires are signal ground (SG) and signal battery (SB). In Type II, SG and SB are the return paths for the E-lead and M-lead respectively.

The Type II interface exists for applications where a common ground between the PBX and the Cisco voice equipment (tie-line equipment) is not possible or practical; for example, the PBX is in one building on a campus and the Cisco equipment is in another. Because there is no common ground, each of the signals has its own return. For the E signal, the tie-line equipment permits the current to flow from the PBX; the current returns to the PBX SG lead or reference. Similarly, the PBX closes a path for the current to generate the M signal to the Cisco voice equipment (tie-line equipment) on the SB lead.



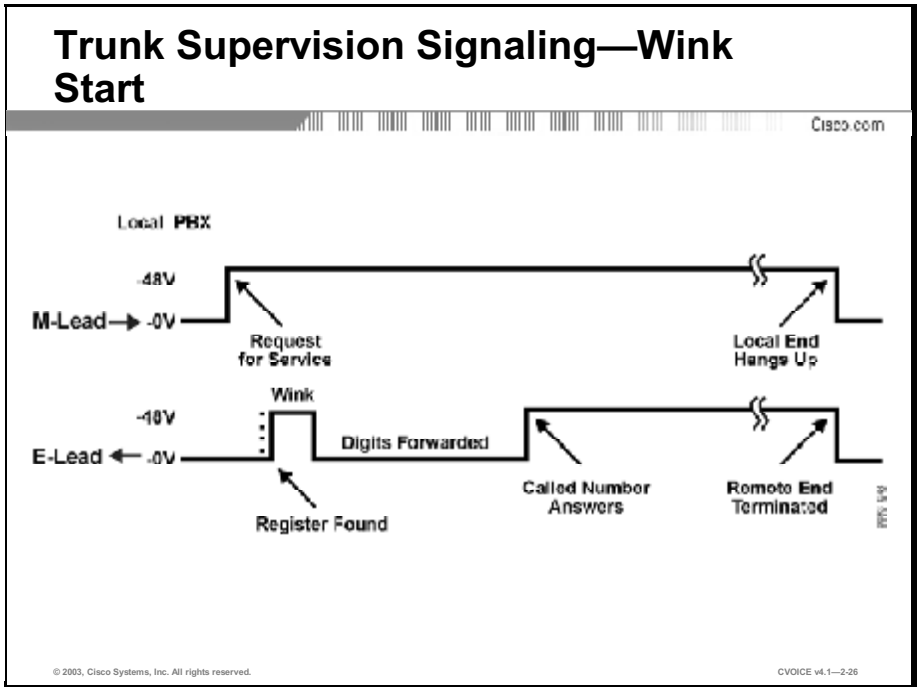
Type III is useful for environments where the M-lead is likely to experience electrical interference and falsely signal its attached equipment. When idle, Type III latches the M-lead via an electrical relay to the SG lead. When the PBX activates the M-lead, it first delatches the SG lead via the relay and signals normally, as in Type II. Type III is not a common implementation.



Type IV is a variation of Type II. In this arrangement, the battery source and ground are reversed on the SB and M wires (as compared to Type II). This means that both the SB and SG wires are grounded. Type IV signaling is symmetric and requires no common ground. Each side closes a current loop to signal, which detects the flow of current through a resistive load to indicate the presence of the signal. Cisco voice equipment does not support Type IV.

Trunk Signal Types Used by Ear and Mouth

This topic describes Wink-Start, immediate start, and delay-start signaling as used by E&M signaling.

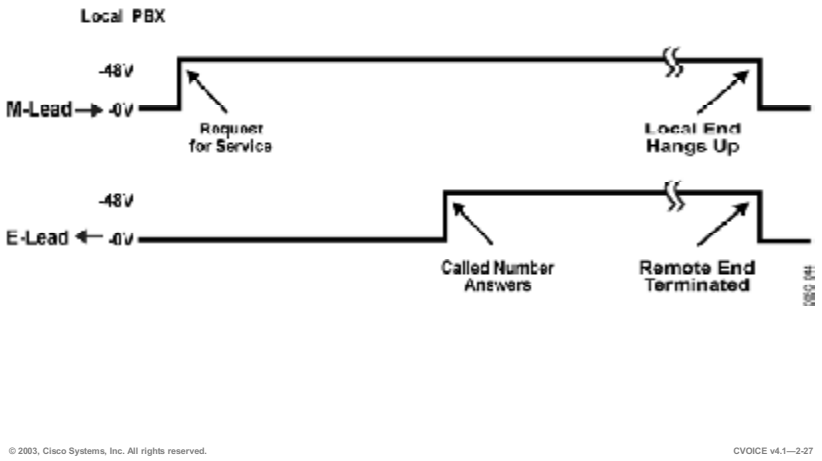


Tie trunks have bidirectional supervision signaling that allows either end to initiate a trunk seizure. In this way, one PBX seizes the trunk, which then waits for an acknowledgment reply from the remote end. The local end must differentiate between a return acknowledgment and a remote-end request for service. Wink-Start signaling is the most common E&M trunk seizure signal type.

The following scenario summarizes the Wink-Start protocol event sequence:

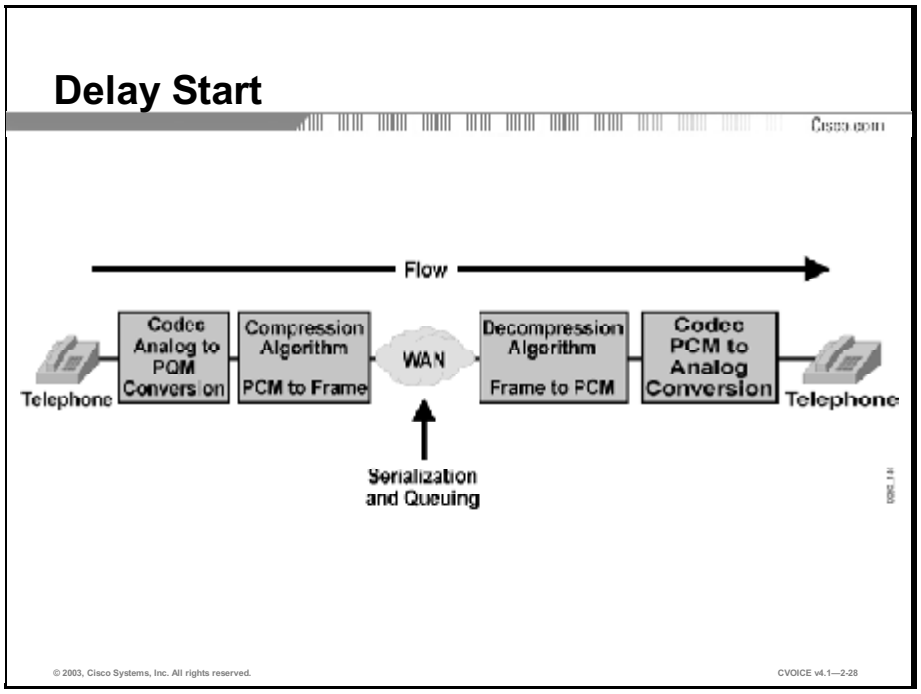
1. The calling office seizes the line by activating its M-lead.
2. Instead of returning an off-hook acknowledgment immediately, the called switch allocates memory for use as a dial register, in the area of memory it uses to store incoming digits.
3. The called switch toggles its M-lead *on* and *off* for a specific time (usually 170 to 340 ms). (This on-hook/off-hook/on-hook sequence constitutes the *wink*.)
4. The calling switch receives the wink on its E-lead and forwards the digits to the remote end. DTMF tones are forwarded across the E&M link in the audio path, not on the M-lead.
5. The called party answers the telephone, and the called PBX raises its M-lead for the duration of the call.

Trunk Supervision Signaling—Immediate Start



If the timing of the returned wink is too short or impossible to detect, the trunk uses immediate start. This occurs occasionally if a PBX vendor implements Wink Start but does not conform to the standards. The following scenario summarizes the sequence of events for the immediate-start protocol:

1. The calling PBX seizes the line by activating its M-lead.
2. Instead of receiving an acknowledgment, the calling PBX waits a predetermined period of time (a minimum of 150 ms) and forwards the digits blindly. DTMF tones are forwarded across the E&M link in the audio path, not on the M-lead
3. The called PBX acknowledges the calling PBX only after the called party answers the call by raising its M-lead.



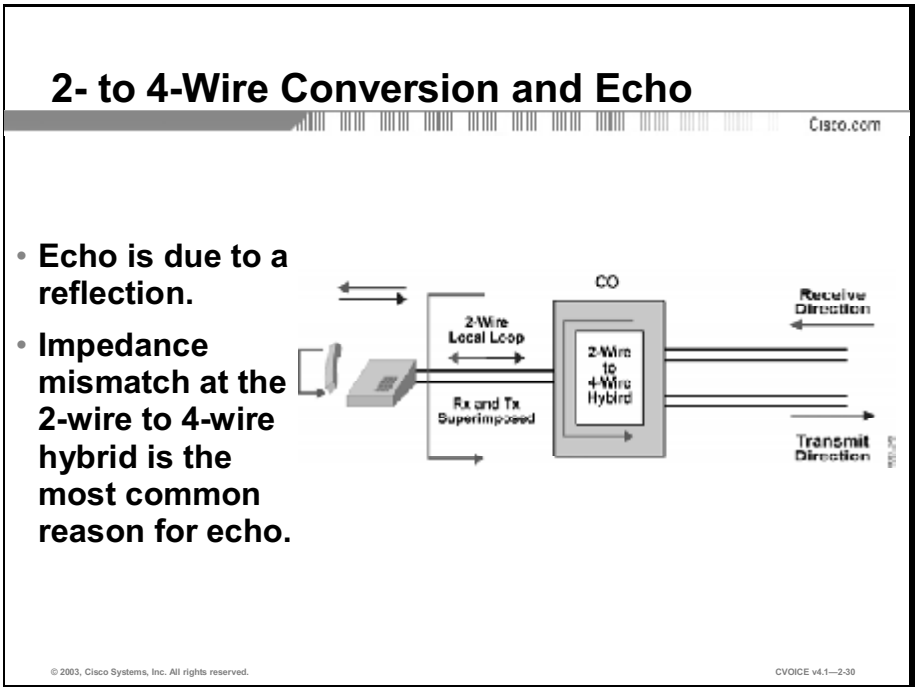
Overall or absolute delay can also add to line quality problems. Encoding, compression, queuing, serialization, and WAN framing and switching delays all add up to overall delay.

Delay start is the original start protocol for E&M. It is used when all of the equipment is mechanical and requires time to process requests. The following scenario summarizes delay-start signaling:

1. When you place a call, your calling switch goes off hook by activating its M-lead.
2. The called switch acknowledges the request by activating its M-lead, and then rotates armatures and gears to reset its dial register to zero.
3. When the dial register at the called switch is in the ready state, the called switch deactivates its M-lead.
4. The calling switch then sends dialed digits. DTMF tones are forwarded across the E&M link in the audio path, not on the M-lead.
5. When the called party answers, the called switch again activates its M-lead.

Line Quality

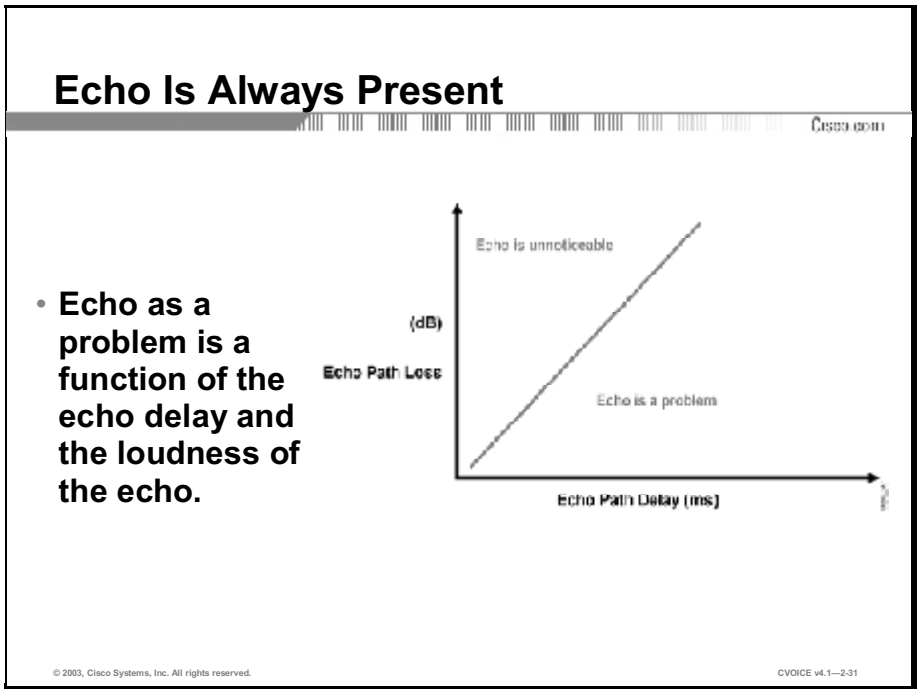
This section describes impairments commonly found in analog telephone circuits and offers solutions to the problem of echo.



Although a local loop consists of two wires, when it reaches the switch, the connection changes to four wires with a two- to four-wire hybrid converter. Trunks then transport the signal across the network.

Telephone networks can experience two types of echo: acoustic echo and electrical echo. Acoustic echo frequently occurs with speakerphones when the received voice on the speaker excites the microphone and travels back to the speaker. Electrical echo occurs when there is an electrical inconsistency in the telephony circuits. This electrical inconsistency is called *impedance mismatch*.

If the lines have a good impedance match, the hybrid is considered “balanced,” with little or no reflected energy. However, if the hybrid is inadequately balanced, and a portion of the transmit voice is reflected back toward the receive side, echo results.



Some form of echo is always present. However, echo can become a problem when:

- Its magnitude or loudness is high.
- The delay time between when you speak and when you hear your voice reflected is significant.

The two components of echo are loudness and delay. Reducing either component reduces overall echo.

Note	Echo is also a problem in situations where the listener hears the speaker twice.

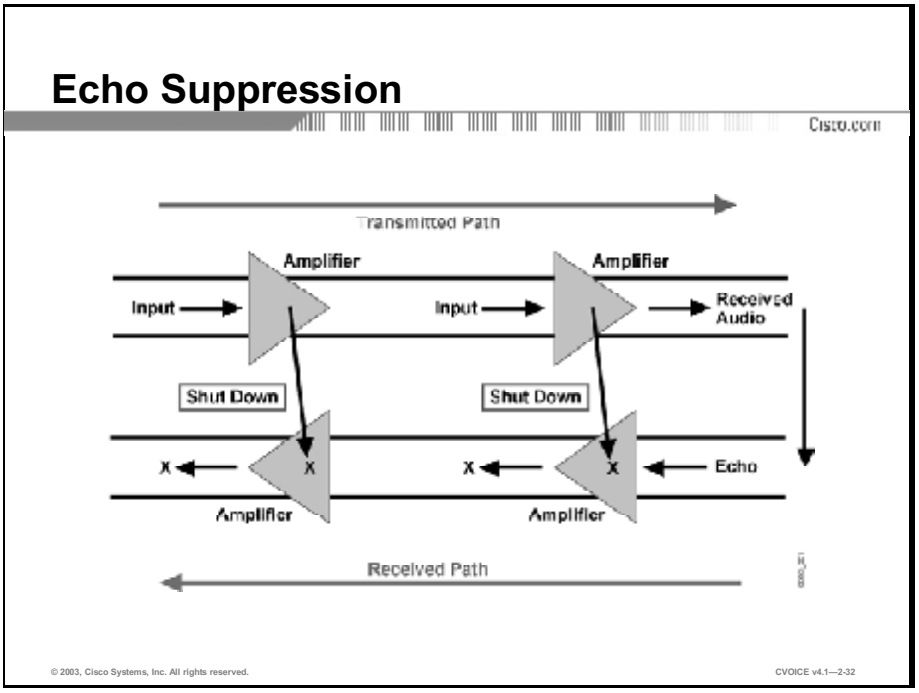
Note	Echo tolerance varies. For most users, however, echo delay over 50 ms is generally problematic.

Example

When a user experiences delay, the conversation can get choppy, and the words of the participants sometimes overlap.

Management of Echo

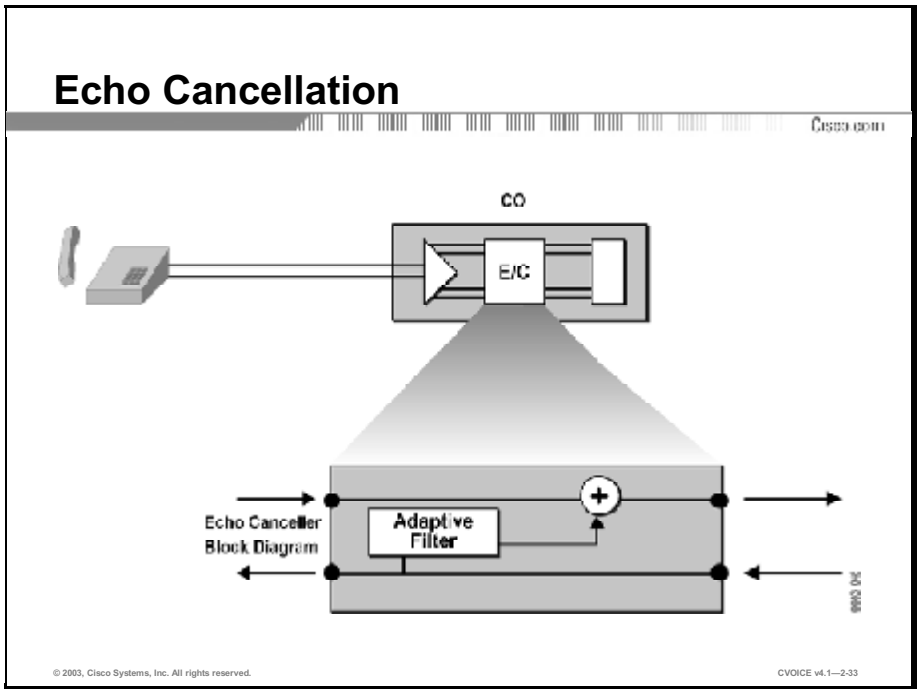
This section explains and compares the two approaches to echo management.



There are two ways to solve an echo problem in your telephone network:

- Echo suppression
- Echo cancellation

The echo suppressor works by transmitting speech in the forward direction and prohibiting audio in the return direction. The echo suppressor essentially breaks the return transmission path. This solution works sufficiently for voice transmission; for full-duplex modem connections, however, the action of the echo suppressor prevents communication. Therefore, when modems “handshake,” the answering modem returns a tone of 2025 Hz to the calling modem, which serves to disable the echo suppressors along the transmission path.



Echo suppression has shortcomings in addressing certain echo conflict situations. Echo cancellation is a more sophisticated method of eliminating echo.

Rather than breaking or attenuating the return path (as in echo suppression), echo cancellation uses a special circuit to build a mathematical model of the transmitted speech pattern and subtract it from the return path. This echo elimination method is depicted in the figure.

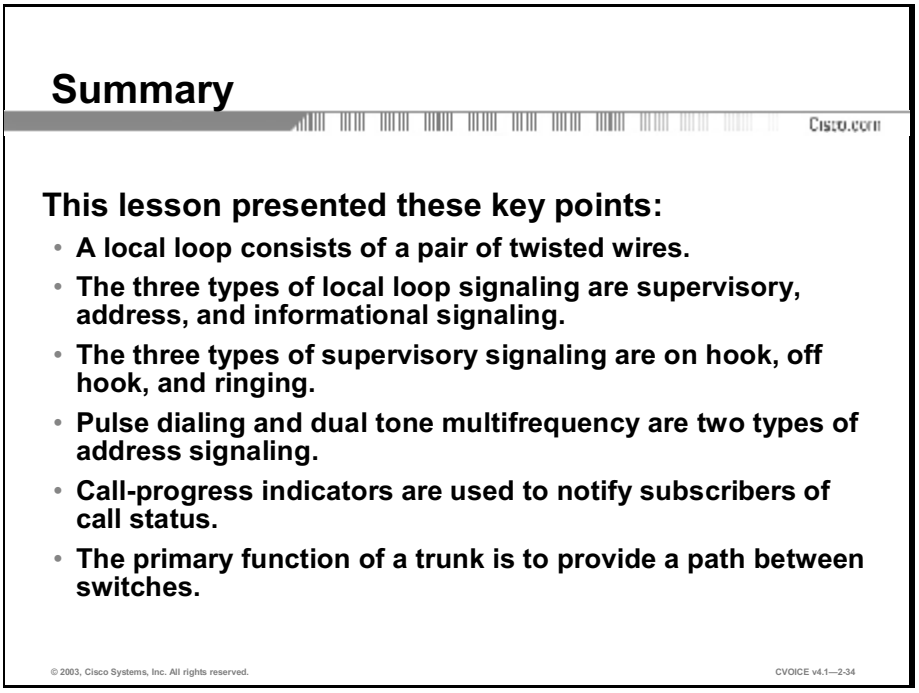
Note	Echo cancellation applies the same technology that is used in audio headphones to cancel ambient noise.

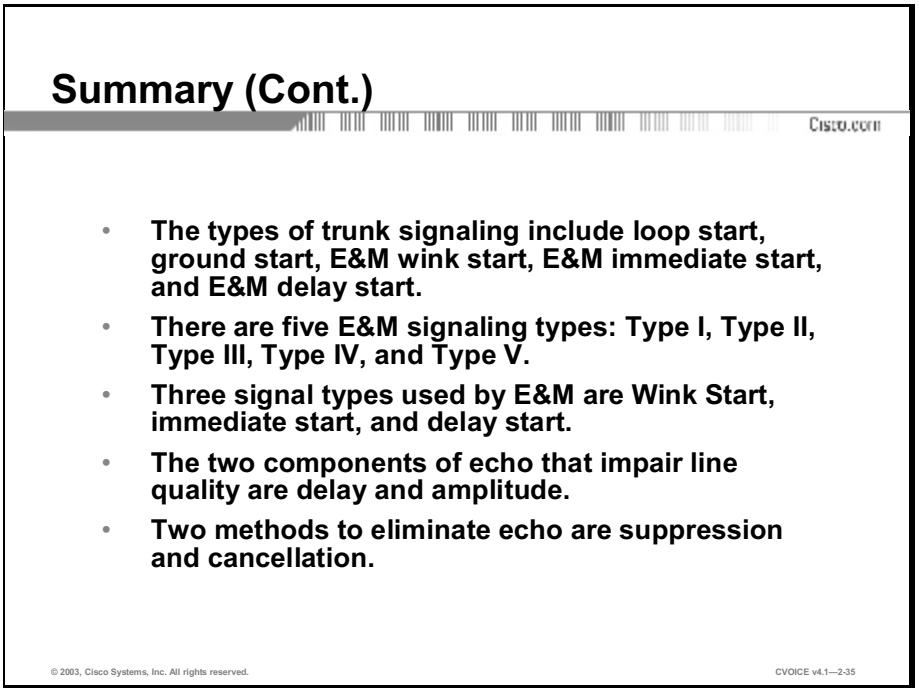
Echo cancellation is the most common method of removing echo in the telephone network today. Echo cancellation is used when it is necessary to adjust for echo on a Cisco device.

Note	The echo canceller removes the echo from one end of the circuit only. If echo is an issue at both ends of the circuit, you must apply another echo canceller at the other end.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Analog Voice Basics
- Assessment (Complex Lab): Refer to Lab 2-1, contained in Laboratory Exercises in Additional Resources section E.
- Analog to Digital Voice Encoding lesson

References

For additional information, refer to these resources:

- Cisco Press “Cisco Voice over Frame Relay, ATM, and IP”, ISBN # 1-57870-227-5

Quiz: Analog Voice Basics

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Identify the components of local-loop connections
- Identify the signaling used on local loops
- Identify on-hook, off-hook, and ringing-supervisory signaling
- Identify pulse dialing and dual tone multifrequency
- List the call-progress indicators and their functions
- State the purpose and types of trunk connections
- Identify the signaling used on trunks
- Identify the five types of wiring schemes used in ear and mouth signaling
- Describe Wink-Start, immediate-start, and delay-start signaling
- Describe impairments that interfere with line quality
- Identify two methods that are used in the industry to reduce the problem of echo

Instructions

Answer these questions.

Q1) In most local-loop connections, what does the ring wire tie to?

A) battery

B) ground

C) telephone

D) switch

Q2) What allows the current to flow around the loop?

A) when the ring wire connects to the negative side of a power source

B) when the tip wire connects to the ground

C) when the telephone goes off hook

D) when the telephone goes on hook

Q3) What are the three different types of local-loop signaling? (Choose three.)

A) address signaling

B) coding signaling

C) control signaling

D) informational signaling

E) remote signaling

F) supervisory signaling

Q4) What two tools do subscriber and telephone companies use to notify each other of call status? (Choose two.)

A) audible tones

B) digital signatures

C) electrical current

D) pulse packets

E) tagged packets

Q5) What happens when the switch hook is in a closed state?

A) only the ringer is active

B) the telephone is on hook

C) the current flows through the electrical loop

D) the current cannot flow through the electrical loop

Q6) What is the ringing tone in the United States?

A) one 2-second tone followed by 2 seconds of silence

B) one 2-second tone followed by 4 seconds of silence

C) two 0.4-second rings separated by 0.2 seconds of silence, followed by 2 seconds of silence

D) two 2-second rings separated by 4 seconds of silence

Q7) In the United States, what is the required ratio of the break/make cycle for rotary-dial telephones?

A) 60-percent break to 40-percent make

B) 60-percent make to 40-percent break

C) 80-percent break to 20-percent make

D) 80-percent make to 20-percent break

Q8) On a DTMF phone, each button on the keypad is associated with _____.

A) a series of pulses

B) a set of dial tones

C) a make and break cycle

D) a set of high and low frequencies

Q9) Which call progress indicator is used to let you know that the telephone company is working on completing the call?

A) busy

B) confirmation tone

C) dial tone

D) ringback

Q10) Which tone is used to indicate that all the local telephone circuits are busy?

A) busy

B) ringback

C) all circuits busy

D) reorder

Q11) Match the trunk type with its description.

A) private trunk lines

B) CO trunks

C) interoffice trunks

D) FX trunks

_____ 1. trunk interfaces that connect to station equipment or office equipment

_____ 2. trunk circuit that connects two local telephone company COs

_____ 3. direct connection between a PBX and the local CO

_____ 4. dedicated circuits that connect PBXs

Q12) What type of trunk is required on a home telephone?

A) private tie-line

B) CO trunk

C) interoffice trunk

D) FX trunk

Q13) Which statement describes the problem of glare in loop-start signaling?

A) The trunk is simultaneously seized from both ends.

B) The signal is so loud that it cannot be understood.

C) The trunk is overloaded with too many messages.

D) The ring voltage is so high that it interferes with communication.

Q14) Which trunk signaling method uses separate wires for voice and signaling?

A) loop start

B) ground start

C) E&M

D) CAS

Q15) Which E&M signaling type is not supported by Cisco voice equipment?

A) Type I

B) Type II

C) Type III

D) Type IV

E) Type V

Q16) Which type of E&M signaling is useful when the PBX and the Cisco equipment are in different buildings on the campus?

A) Type I

B) Type II

C) Type III

D) Type IV

E) Type V

Q17) Which type of E&M signaling is used when all the equipment is mechanical?

A) Wink Start

B) immediate start

C) delay start

Q18) Which type of E&M signaling is the most commonly used?

A) Wink Start

B) immediate start

C) delay start

Q19) How much echo delay is generally not problematic?

A) below 50 ms

B) below 100 ms

C) below 120 ms

D) below 150 ms

Q20) Which two factors contribute to echo problems? (Choose two.)

A) attenuation

B) crosstalk

C) delay

D) electric current on the line

E) incorrect voltage

F) loudness

Q21) Which method is used to reduce echo on Cisco devices?

A) echo suppression

B) echo cancellation

C) echo correction

D) echo return loss

Q22) In what situations is it problematic to use echo suppression?

A) for voice transmission

B) for half-duplex modem connections

C) for full-duplex modem connections

D) all of the above

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Analog to Digital Voice Encoding

Overview

This lesson covers the fundamentals of digital voice encoding. You will learn the basics of voice digitization and the various compression schemes that are used to transport voice using less bandwidth. You will also learn about voice quality measurement techniques to help you choose the compression scheme that best suits your needs.

Importance

To deploy Voice over IP (VoIP) networks, the voice must be digitized. Understanding how voice digitization works and what compression schemes are offered helps you to understand the bandwidth requirements for each type of compression.

Objectives

Upon completing this lesson, you will be able to:

- Identify the steps for converting analog signals to digital signals
- Identify the steps for converting digital signals to analog signals
- State the purpose of the Nyquist Theorem
- Explain quantization
- Name two types of voice compression techniques
- Describe the similarities and differences of G.729 and G.729A compression

- List three common voice compression standards and their bandwidth requirements
- State the purpose of voice quality measurement and the method of calculation for each type of measurement

Learner Skills and Knowledge

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

- Understanding of analog voice telephony
- Familiarity with PBXs and voice switches
- Understanding of analog voice signaling

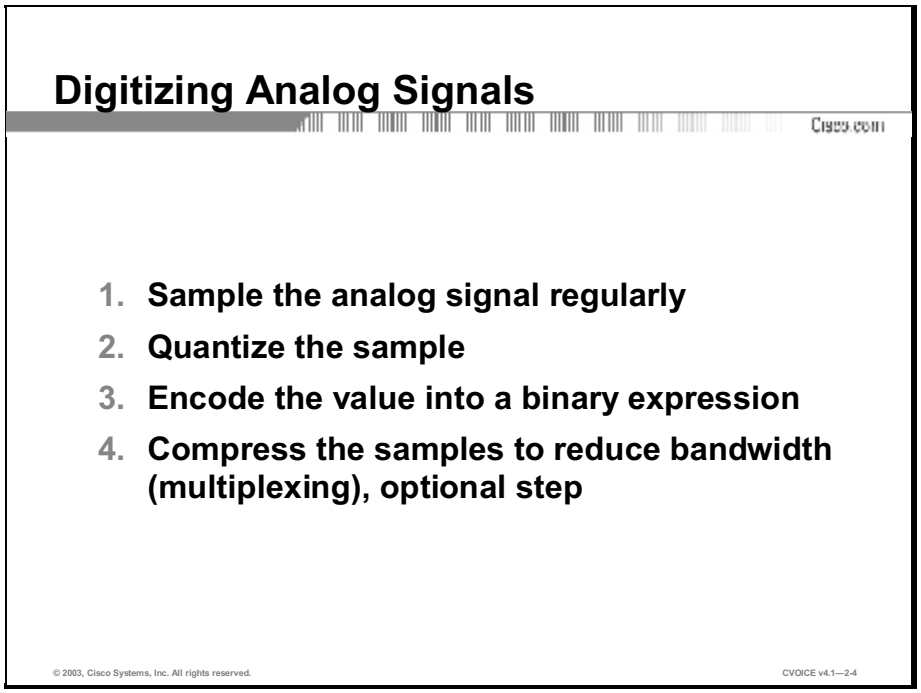
Outline

This lesson includes these topics:

- Overview
- Basic Voice Encoding: Converting Analog to Digital
- Basic Voice Encoding: Converting Digital to Analog
- The Nyquist Theorem
- Quantization
- Voice Compression and Coder-Decoder Standards
- G.729 and G.729A Compared
- Compression Bandwidth Requirements
- Voice Quality Measurement
- Summary
- Assessment (Quiz): Analog to Digital Voice Encoding
- Assessment (Complex Lab): Lab Exercise 2-1

Basic Voice Encoding: Converting Analog to Digital

This topic describes the process of converting analog signals to digital signals.



Digitizing speech was a project first undertaken by the Bell System in the 1950s. The original purpose of digitizing speech was to deploy more voice circuits with a smaller number of wires. This evolved into the T1 and E1 transmission methods of today.

To convert an analog signal to a digital signal, you must perform these steps:

Note	The last step is optional.

Table 1: Analog to Digital Signal Conversion

Step	Procedure	Description
1.	Sample the analog signal regularly.	The sampling rate must be two times the highest frequency to produce playback that appears neither choppy nor too smooth.
2.	Quantize the sample.	Quantization consists of a scale made up of 8 major divisions or chords. Each chord is subdivided into 16 equally spaced steps. The chords are not equally spaced but are actually finest near the origin. Steps are equal within the chords but different when they are compared between the chords. Finer graduations at the origin result in less distortion for low-level tones.
3.	Encode the value into 8-bit digital form.	PBX output is a continuous analog voice waveform. T1 digital voice is a snapshot of the wave encoded in ones and zeros.
4.	(Optional) Compress the samples to reduce bandwidth.	Although not essential to convert analog signals to digital, signal compression is widely used to reduce bandwidth.

To avoid potential aliasing conflicts during the encoding or decoding process, you must use a band-pass filter to restrict voice signals to a 300-Hz to 3400-Hz range

Three components in the analog-to-digital conversion process include:

- **Sampling:** Sample the analog signal at periodic intervals. The output of sampling is a pulse amplitude modulation (PAM) signal.

- **Quantization:** Match the PAM signal to a segmented scale. This scale measures the amplitude (height) of the PAM signal and assigns an integer number to define that amplitude.

- **Encoding:** Convert the integer base-10 number to a binary number. The output of encoding is a binary expression in which each bit is either a 1 (pulse) or a 0 (no pulse).

This three-step process is repeated 8000 times per second for telephone voice channel service. Use the fourth optional step—compression—to save bandwidth. This optional step allows a single channel to carry more voice calls.

Note The most commonly used method of converting analog to digital is pulse code modulation (PCM).

Basic Voice Encoding: Converting Digital to Analog

This topic describes the process of converting digital signals back to analog signals.

After the receiving terminal at the far end receives the digital PCM signal, it must convert the PCM signal back into an analog signal.

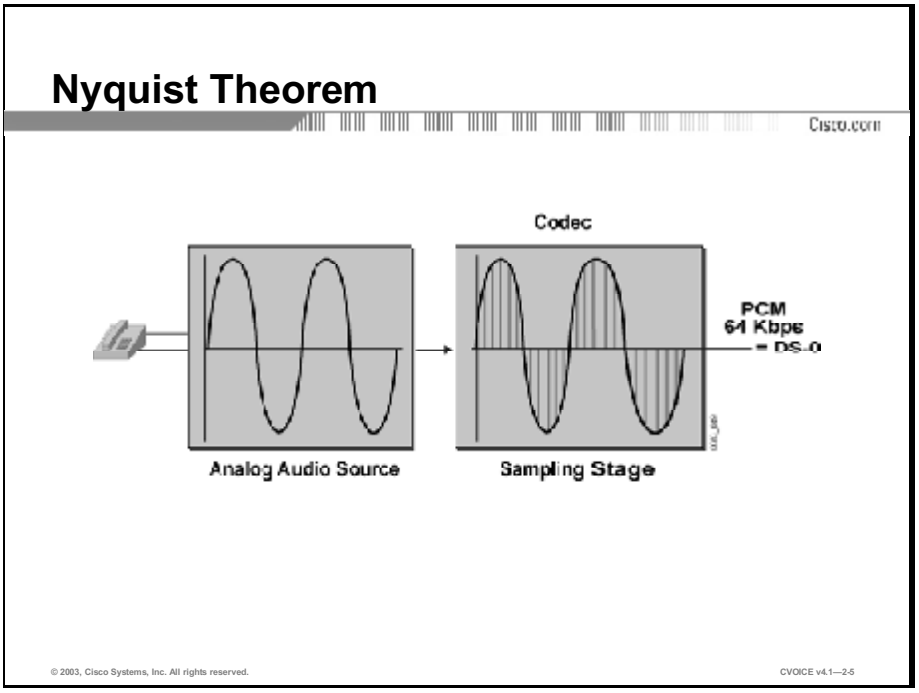
The process of converting digital signals back into analog signals includes the following two parts:

- **Decoding:** The received eight-bit word is decoded to recover the number that defines the amplitude of that sample. This information is used to rebuild a PAM signal of the original amplitude. This process is simply the reverse of the analog-to-digital conversion.

- **Filtering:** The PAM signal is passed through a properly designed filter that reconstructs the original analog wave form from its digitally coded counterpart.

The Nyquist Theorem

This topic describes the Nyquist Theorem that is the basis for digital signal technology.



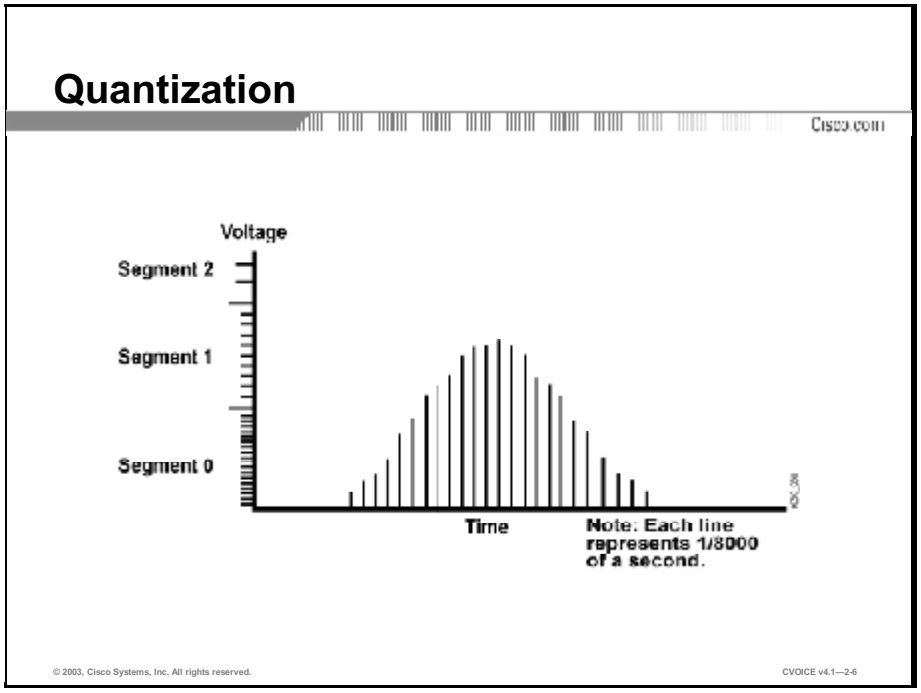
Digital signal technology is based on the premise stated in the Nyquist Theorem: when a signal is instantaneously sampled at the transmitter in regular intervals and has a rate of at least twice the highest channel frequency, then the samples will contain sufficient information to allow an accurate reconstruction of the signal at the receiver.

Example

While the human ear can sense sounds from 20 to 20,000 Hz, and speech encompasses sounds from about 200 to 9000 Hz, the telephone channel was designed to operate at about 300 to 3400 Hz. This economical range carries enough fidelity to allow callers to identify the party at the far end and sense their mood. Nyquist decided to extend the digitization to 4000 Hz, to capture higher-frequency sounds that the telephone channel may deliver. Therefore, the highest frequency for voice is 4000 Hz, or 8000 samples per second; that is, one sample every 125 microseconds.

Quantization

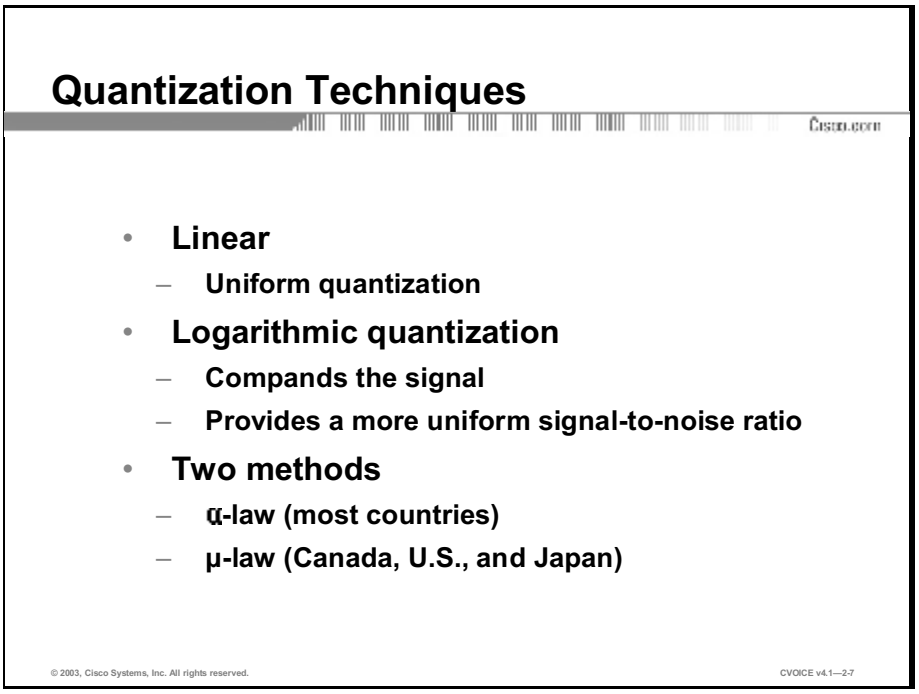
This topic explains quantization and its techniques.



Quantization involves dividing the range of amplitude values that are present in an analog signal sample into a set of discrete steps that are closest in value to the original analog signal. Each step is assigned a unique digital code word.

The figure here depicts quantization. In this example, the x-axis is time and the y-axis is the voltage value (PAM).

The voltage range is divided into 16 segments (0 to 7 positive, and 0 to 7 negative). Starting with segment 0, each segment has fewer steps than the previous segment, which reduces the noise-to-signal ratio and makes it uniform. This segmentation also corresponds closely to the logarithmic behavior of the human ear. If there is a noise-to-signal ratio problem, it is resolved by using a logarithmic scale to convert PAM to PCM.



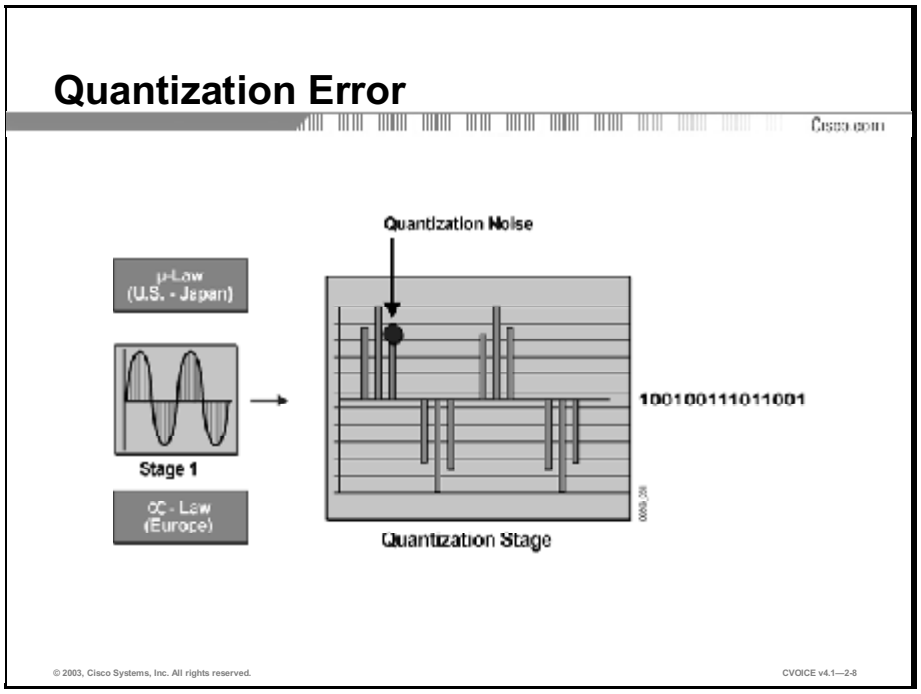
Linear sampling of analog signals cause small-amplitude signals to have a higher noise-to-signal ratio, and therefore poorer quality than larger amplitude signals. The Bell System developed the *μ-law* method of quantization, which is widely used in North America. The International Telecommunication Union (ITU) modified the original μ-law method and created *α-law*, which is used in countries outside of North America.

By allowing smaller step functions at lower amplitudes—rather than higher amplitudes—μ-law and α-law provide a method of reducing this problem. Both μ-law and α-law compand the signal; for example, they both compress the signal for transmission and then expand the signal back to its original form at the other end.

To calculate the bit rate of digital voice, you must use this formula:

- 2 x 4 kHz x 8 bits per sample = 64,000 bits per second (64 kbps). 64 kbps is a DS-0 rate.

The result of using μ-law and α-law is a more accurate value for smaller amplitude and uniform signal-to-noise quantization ratio (SQR) across the input range



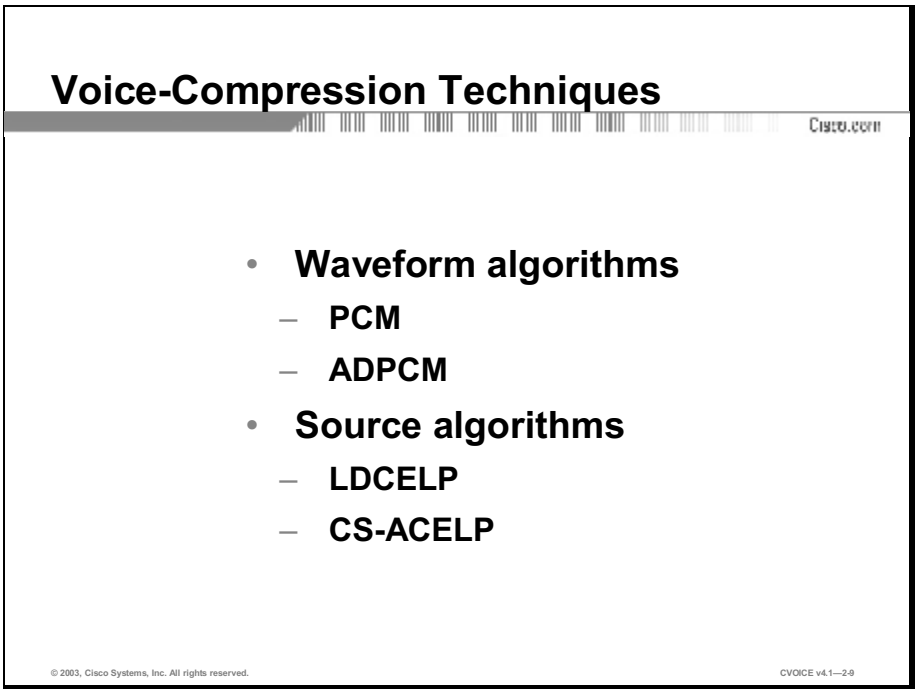
Both μ-law and A-law are linear approximations of a logarithmic input/output relationship. They both generate 64-kbps bit streams using 8-bit code words to segment and quantize levels within segments.

The difference between the original analog signal and the quantization level assigned is called quantization error, which is the source of distortion in digital transmission systems. Quantization error is any random disturbance or signal that interferes with the quality of the transmission or the signal itself.

Note	For communication between a μ-law country and an A-law country, the μ-law country must change its signaling to accommodate the A-law country.

Voice Compression and Coder-Decoder Standards

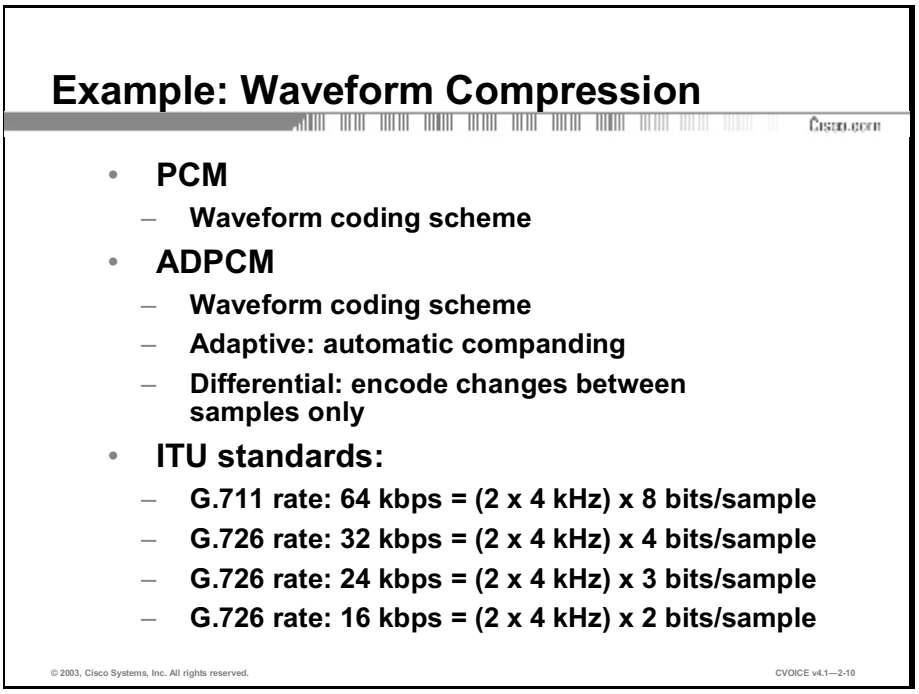
This topic describes two types of speech-coding schemes: waveform and source coding.



There are two voice compression techniques:

- Waveform algorithms (coders) function as follows:
  - Sample analog signals at 8000 times per second
  - Use predictive differential methods to reduce bandwidth
  - Bandwidth reduction highly impacts voice quality
  - Do not take advantage of speech characteristics
- Source algorithms function as follows:
  - Source algorithm coders are called vocoders. Vocoder is a term that describes ‘Voice Coding’, which is a device that converts analog speech into digital speech, using a specific compression scheme that is optimized for coding human speech.
  - Vocoders take advantage of speech characteristics.
  - Bandwidth reduction occurs by sending transmitting linear-filter settings.

- Codebooks store specific predictive waveshapes of human speech. They match the speech, encode the phrases, decode the waveshapes at the receiver by looking up the coded phrase, and match it to the stored waveshape in the receiver codebook.



Standard PCM is known as ITU standard G.711.

Adaptive differential pulse code modulation (ADPCM) coders, like other waveform coders, encode analog voice signals into digital signals to adaptively predict future encodings by looking at the immediate past. The adaptive feature of ADCPM reduces the number of bits per second that the PCM method requires to encode voice signals.

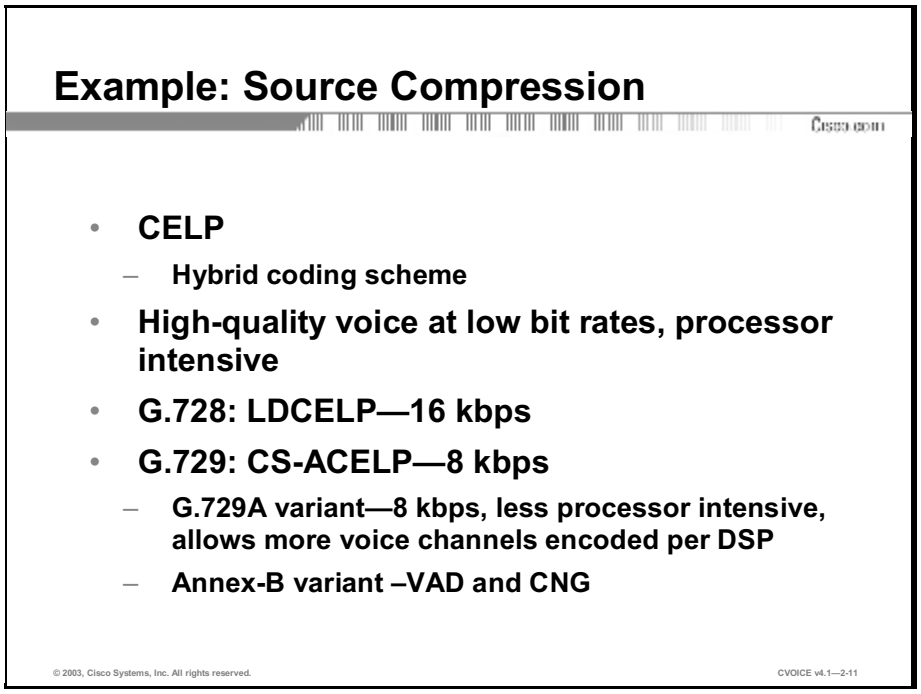
ADCPM does this by taking 8000 samples per second of the analog voice signal and turning them into a linear PCM sample. ADCPM then calculates the predicted value of the next sample, based on the immediate past sample, and encodes the difference. The ADPCM process generates 4-bit words, therefore generating 16 specific bit patterns.

The ADPCM algorithm from the Consultative Committee for International Telegraph and Telephone (CCITT) transmits all 16 possible bit patterns. The ADPCM algorithm from the American National Standards Institute (ANSI) uses 15 of the 16 possible bit patterns. The ANSI ADPCM algorithm does not generate a 0000 pattern.

The ITU standards for compression are as follows:

- **G.711 rate:** 64 kbps = (2 x 4 kHz) x 8 bits/sample
- **G.726 rate:** 32 kbps = (2 x 4 kHz) x 4 bits/sample
- **G.726 rate:** 24 kbps = (2 x 4 kHz) x 3 bits/sample
- **G.726 rate:** 16 kbps = (2 x 4 kHz) x 2 bits/sample

Note CCITT is now called ITU-T.



Code excited linear prediction (CELP) compression transforms analog voice signals as follows:

- The input to the coder is converted from an 8-bit PCM to a 16-bit linear PCM sample.
- A codebook uses feedback to continuously learn and predict the voice waveform.
- The coder is excited by a white noise generator.
- The mathematical result (recipe) is sent to the far-end decoder for synthesis and generation of the voice waveform.

Low-delay CELP (LDCELP) is similar to Conjugate Structure Algebraic Code Excited Linear Prediction (CS-ACELP), except:

- LDCELP uses a smaller codebook and operates at 16 kbps to minimize delay—or look-ahead—to 2 to 5 ms.
- The 10-bit codeword is produced from every five speech samples from the 8-kHz input.
- Four of these 10-bit codewords are called a subframe; they take approximately 2.5 ms to encode.

Two of these subframes are combined into a 5-ms block for transmission. CS-ACELP is a variation of CELP that performs these functions:

- Codes on 80-byte frames, which take approximately 10 ms to buffer and process

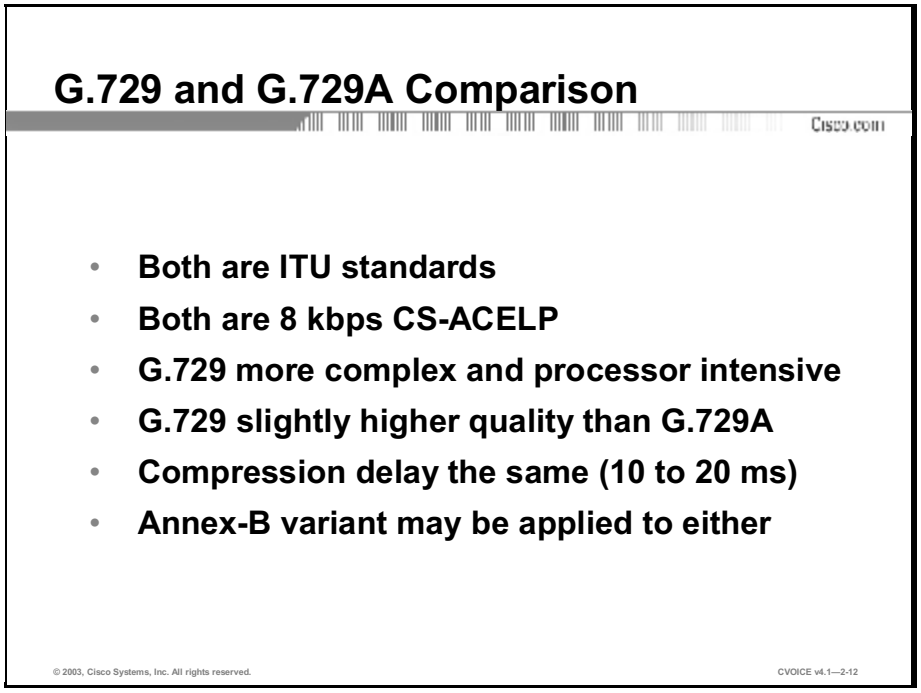
- Adds a look-ahead of 5 ms. A look-ahead is a coding mechanism that continuously analyzes, learns, and predicts the next waveshape.
- Adds noise reduction and pitch-synthesis filtering to processing requirements

Example

The Annex-B variant adds voice activity detection (VAD) in strict compliance with G.729B standards. When this coder-decoder (codec) variant is used, VAD is not tunable for music threshold. However, when Cisco VAD is configured, music threshold is tunable.

G.729 and G.729A Compared

This topic compares G.729 and G.729A compression.



G.729, G.729 Annex-A (G.729A), G.729 Annex-B (G.729B), and G.729A Annex-B (G.729AB) are variations of CS-ACELP.

There is little difference between the ITU recommendations for G.729 and G.729A. All of the platforms that support G.729 also support G.729A.

G.729 is the compression algorithm that Cisco uses for high-quality 8-kbps voice. When properly implemented, G.729 sounds as good as the 32-kbps ADPCM. G.729 is a high-complexity, processor-intensive, compression algorithm that monopolizes processing resources.

Although G.729A is also an 8-kbps compression, it is not as processor-intensive as G.729. It is a medium-complexity variant of G.729 with slightly lower voice quality. G.729A is not as high-quality as G.729 and is more susceptible to network irregularities, such as delay, variation, and tandeming. Tandeming causes distortion that occurs when speech is coded, decoded, and then coded and decoded again, much like the distortion that occurs when a videotape is repeatedly copied.

Example

On Cisco IOS® gateways, you must use the variant (G.729 or G.729A) that is related to the codec complexity configuration on the voice card. This variant does not show up explicitly in the Cisco IOS command-line interface (CLI) codec choice. For example, the CLI does not display **g729r8** (alpha code) as a codec option. However, if the voice card is defined as medium-complexity, then the **g729r8** option is the G.729A codec.

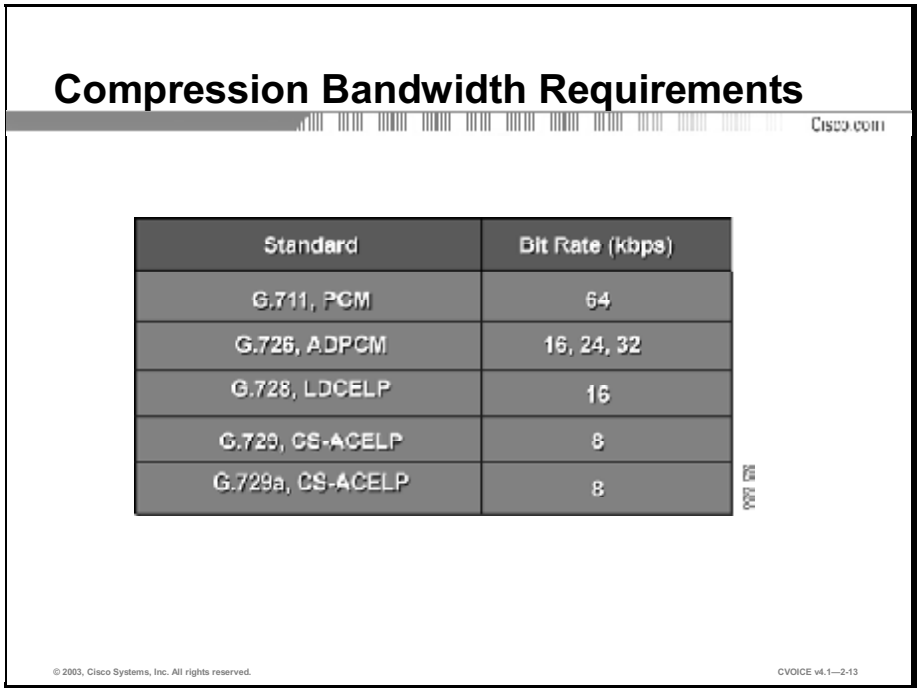
G.729B is a high-complexity algorithm, and G.729AB is a medium-complexity variant of G.729B with slightly lower voice quality. The difference between the G.729 and G.729B codec is that the G.729B codec provides built-in Internet Engineering Task Force (IETF) VAD and comfort noise generation (CNG).

The following G.729 codec combinations interoperate:

- G.729 and G.729A
- G.729 and G.729
- G.729A and G.729A
- G.729B and G.729AB
- G.729B and G.729B
- G.729AB and G.729AB

Compression Bandwidth Requirements

This topic lists the bandwidth requirements for various ITU compression standards.



Three common voice compression techniques are standardized by the International Telecommunication Union Telecommunication Standardization Section (ITU-T) and assigned a number as listed:

- **PCM:** Amplitude of voice signal is sampled and quantized at 8000 times per second. Each sample is then represented by one octet (8 bits) and transmitted. For sampling, you must use either α-law or μ-law to reduce the noise-to-signal ratio.

- **ADPCM:** The difference between the current sample and its predicted value (based on past samples). ADPCM is represented by two, three, four, or five bits. This method reduces the bandwidth requirement at the expense of signal quality.

- **CELP:** Excitation value and a set of linear-predictive filters (settings) are transmitted. The filter setting transmissions are less frequent than excitation values and are sent on an as-needed basis.

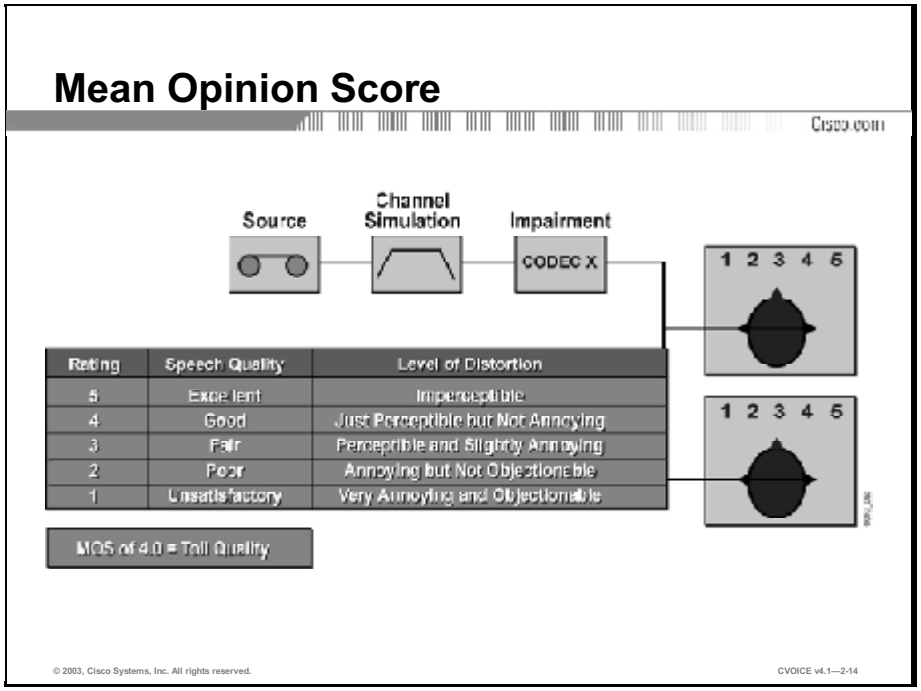
The table describes the codecs and compression standards:

Table 2: Codecs and Compression Standards

Codec	Compression Technique	Bit Rate (kbps)
G.711	PCM	64
G.726	ADPCM	16, 24, 32, 40
G.728	LDCELP	16
G.729	CS-ACELP	8
G.729A	CS-ACELP	8

Voice Quality Measurement

This topic describes two methods that are used to subjectively measure the quality of voice transported on a telephone line. Because different compression schemes produce different quality results, a method of comparing them is necessary.

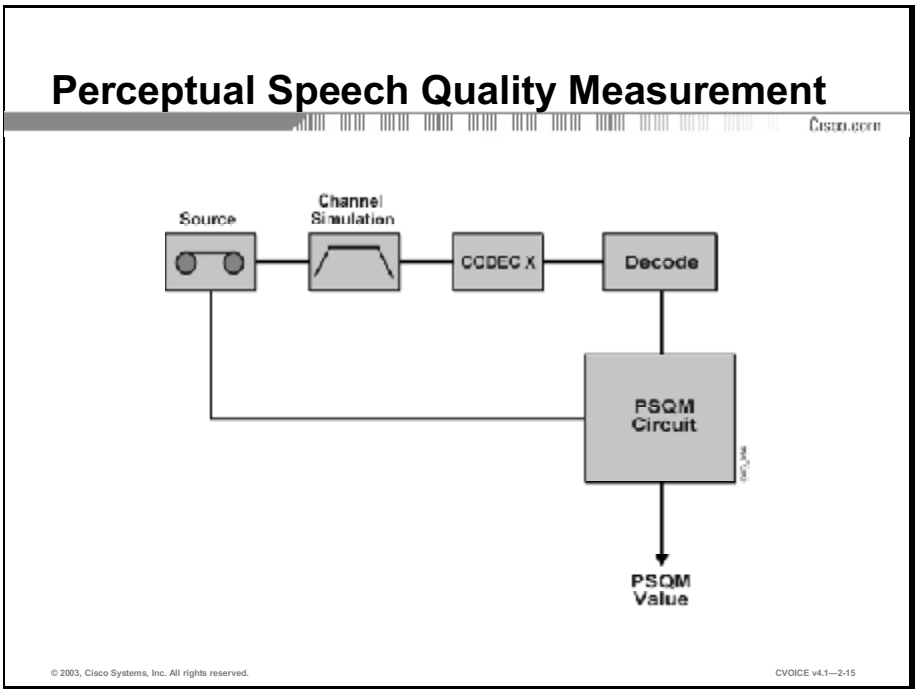


The figure depicts mean opinion score (MOS). MOS is a system of grading the voice quality of telephone connections. The MOS is a statistical measurement of voice quality derived from the judgments of several subscribers.

Graded by humans and very subjective, the range of MOS is 1 to 5, where 5 is direct conversation.

Table 3: Voice Quality of Telephone Connections

Rating	Speech Quality	Level of Distortion
5	Excellent	Imperceptible
4	Good	Just perceptible but not annoying
3	Fair	Perceptible and slightly annoying
2	Poor	Annoying but not objectionable
1	Unsatisfactory	Very annoying and objectionable



A newer, more objective measurement is available that is quickly overtaking MOS scores as the industry quality measurement of choice for coding algorithms. Perceptual Speech Quality Measurement (PSQM), as per ITU standard P.861, provides a rating on a scale of 0 to 6.5, where 0 is best and 6.5 is worst.

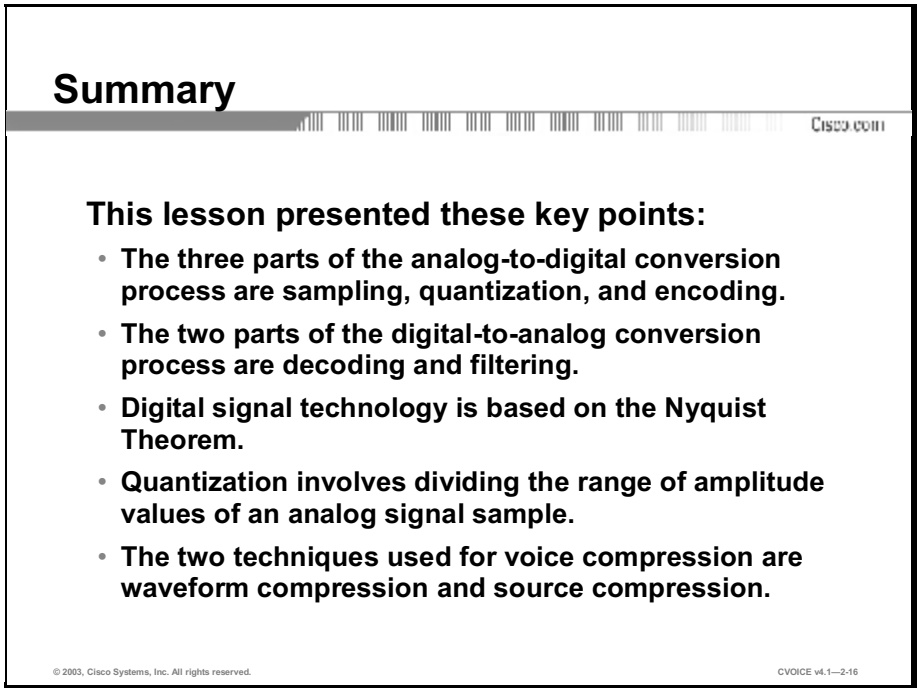
PSQM is implemented in test equipment and monitoring systems that are available from vendors other than Cisco. Some PSQM test equipment converts the 0-to-6.5 scale to a 0-to-5 scale to correlate to MOS. PSQM works by comparing the transmitted speech to the original input and yields a score. Various vendor test equipment is now capable of providing a PSQM score for a test voice call over a particular packet network.

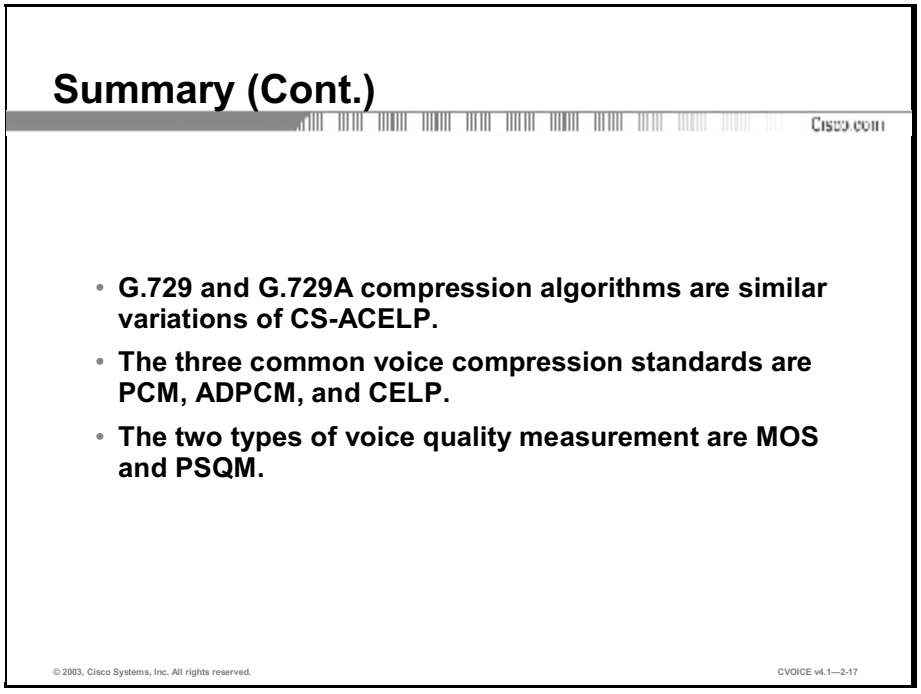
In 1998, British Telecom developed a predictive voice quality measurement algorithm called Perceptual Analysis Measurement System (PAMS). PAMS can predict subjective speech quality measurement methods, such as MOS, when fidelity is affected by such things as waveform codecs, vocoders, and various speaker dependencies, such as language. PAMS, unlike PSQM, includes automatic normalization for levels.

ITU standard P.862 supercedes P.861 and describes a voice quality measurement technique that combines PSQM and PAMS. Originally developed by KPN Research, the Netherlands, and British Telecommunications (BT), Perceptual Evaluation of Speech Quality (PESQ) is an objective measuring tool that can “predict” results of subjective measuring tests, such as MOS. PESQ can be found in test equipment from a variety of vendors.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Analog to Digital Voice Encoding
- Assessment (Complex Lab): Refer to Lab 2-1, contained in Laboratory Exercises in Additional Resources section E.
- Signaling Systems lesson

References

For additional information, refer to these resources:

- Cisco Press “Cisco Voice Over Frame Relay, ATM, and IP”, ISBN# 1-57870-227-5

Quiz: Analog to Digital Voice Encoding

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Identify the steps for converting analog signals to digital signals
- Identify the steps for converting digital signals to analog signals
- State the purpose of the Nyquist Theorem
- Explain quantization
- Name two types of voice compression techniques
- Describe the similarities and differences of G.729 and G.729A compression
- List three common voice compression standards and their bandwidth requirements
- State the purpose of voice quality measurement and the method of calculation for each type of measurement

Instructions

Answer these questions:

Q1) Which of these steps is optional in analog to digital conversion?

A) compression

B) encoding

C) quantization

D) sampling

Q2) How often is the analog to digital signal conversion sampling process repeated for telephone voice channel service?

A) 8000 times per call

B) 8000 times per voice sample

C) 8000 times per second

D) 8000 times per minute

Q3) What device is used to reconstruct the digital signal to its original analog signal?

A) modem

B) compander

C) filter

D) codec

Q4) During the process of converting digital signals back to analog signals, each received 8-bit word is decoded to recover _____.

A) the PAM signal

B) the number that defines the amplitude of the sample

C) the analog wave form

D) the base10 number that corresponds to the 8-bit number

Q5) What frequency range is the telephone channel designed for?

A) 20 to 20,000 Hz

B) 200 to 9000 Hz

C) 300 to 3400 Hz

D) 4000 to 8000 Hz

Q6) If voice is sampled at a rate of one sample every 125 microseconds, what is the highest frequency of sound in the channel according to the Nyquist Theorem?

A) 3400 Hz

B) 4000 Hz

C) 8000 Hz

D) 20,000 Hz

Q7) What is the problem with linear sampling of analog signals?

A) Small-amplitude signals have a higher noise-to-signal ratio.

B) The signal cannot be sampled instantaneously at the transmitter.

C) The sampling interval is too long for high-amplitude signals.

D) The samples do not contain enough information for accurate conversion.

Q8) Which quantization method is used in the United States?

A) α-law

B) μ-law

C) PCM

D) Nyquist

Q9) Which coding schemes are examples of waveform algorithms?

A) PCM

B) ADPCM

C) CELP

D) LDCELP

E) CS-ACELP

Q10) Which is NOT a function of waveform algorithms?

A) sample analog signals at 8000 times per second

B) use predictive differential method to reduce bandwidth

C) use codebooks to match stored waveshapes in the receiver codebook

D) do not take advantage of speech characteristics

Q11) What are the two differences between G.729 and G.729A compression? (Choose two.)

A) the platforms that support them

B) complexity

C) compression delay

D) standards body

E) demands on the processor

Q12) Which two G.729 codecs provides built-in IETF VAD and CNG? (Choose two.)

A) G.729

B) G.729A

C) G.729B

D) G.729AB

E) all of the above

F) none of the above

Q13) Which compression technique is used with G.711 codecs?

A) ADPCM

B) CS-ACELP

C) LDCELP

D) PCM

Q14) Which compression standard has the lowest bandwidth requirement?

A) ADPCM

B) CS-ACELP

C) LDCELP

D) PCM

Q15) What is the level of distortion for a MOS rating of 4?

A) imperceptible

B) just perceptible but not annoying

C) perceptible and slightly annoying

D) annoying but not objectionable

Q16) What is the rating scale for measuring voice quality with PSQM?

A) 1 to 5 where 1 is worst

B) 1 to 5 where 5 is worst

C) 0 to 6.5 where 0 is worst

D) 0 to 6.5 where 6.5 is worst

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Signaling Systems

Overview

This lesson describes the various signaling systems used between telephony systems. This lesson also explores signaling between PBXs, signaling between PBXs and central offices (COs), and specialized signaling, such as ISDN.

Importance

Configuring Cisco Systems voice equipment to interface with other equipment requires an understanding of the signaling that conveys supervision between the systems. Proper troubleshooting also requires an understanding of these signaling systems.

Objectives

Upon completing this lesson, you will be able to:

- State the uses and types of channel associated signaling systems used for T1
- State the uses and types of channel associated signaling systems used for E1
- State the uses and types of common channel signaling systems
- Name the benefits of using ISDN to convey voice
- Name the benefits of using Q Signaling to convey voice
- Name the functions of Signaling System 7 and its benefits
- Describe how separate signaling systems can be interfaced

Learner Skills and Knowledge

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

- Familiarity with PBX systems
- Understanding of the need for signaling between systems
- Understanding of address, supervisory, and call-progress signals

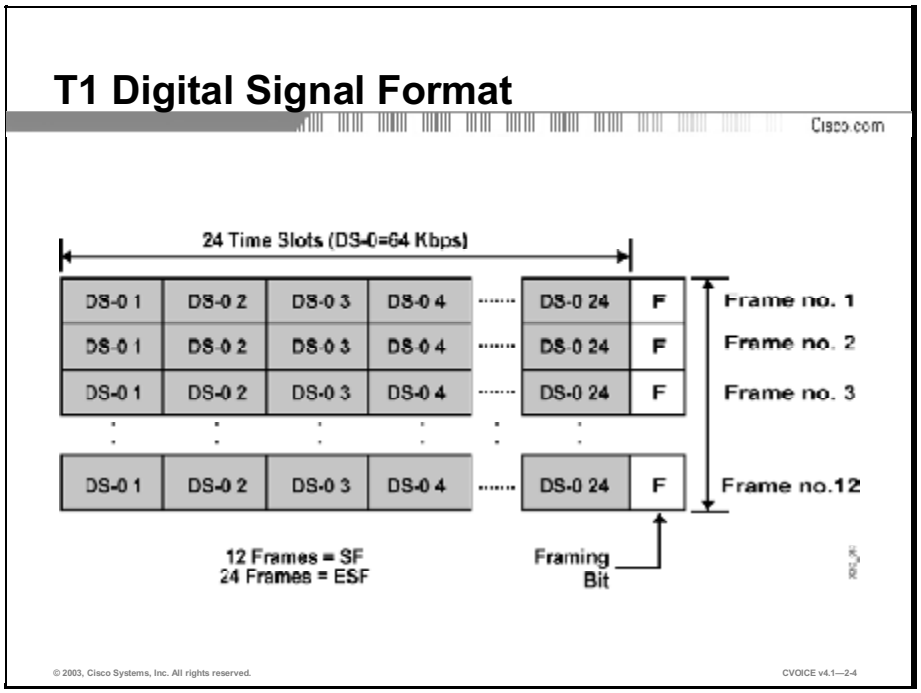
Outline

This lesson includes these topics:

- Overview
- Channel Associated Signaling Systems: T1
- Channel Associated Signaling Systems: E1
- Common Channel Signaling Systems
- ISDN
- Q Signaling
- Signaling System 7
- Signaling Systems Interworking
- Summary
- Assessment (Quiz): Signaling Systems
- Assessment (Complex Lab): Lab Exercise 2-1

Channel Associated Signaling Systems: T1

This topic describes channel associated signaling (CAS) and its uses with T1 transmission. CAS is a signaling method commonly used between PBXs. Although this can manifest itself in many forms, some methods are more common than others. Signaling systems can also be implemented between a PBX and a Cisco voice device.



PBXs and Cisco devices use T1 and E1 to convey voice. Originally, this was the main purpose of T1, which carries signaling information using two methodologies, CAS and common channel signaling (CCS). The figure illustrates the format of the T1 digital signal

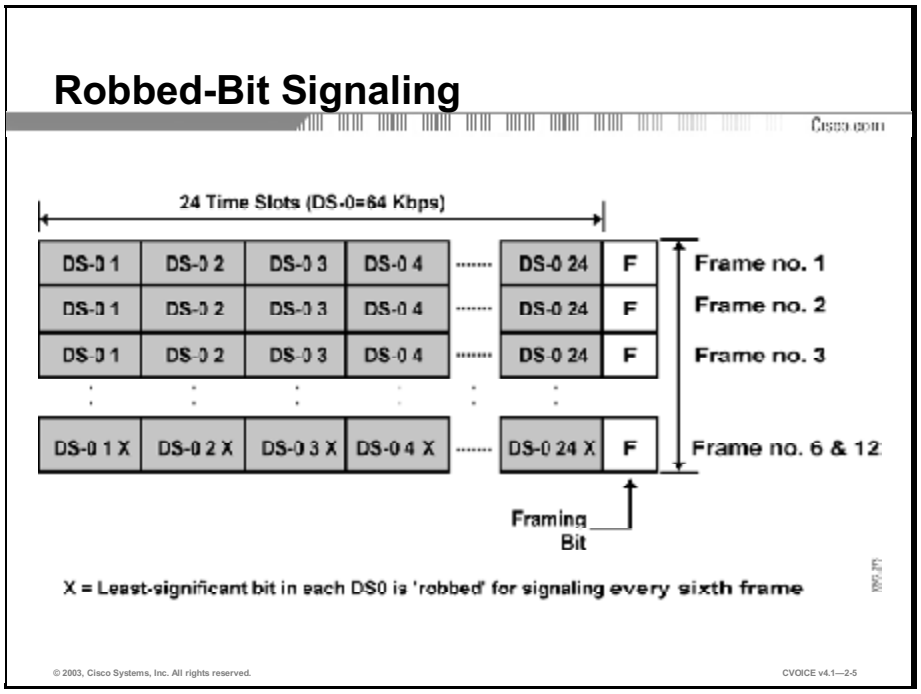
The characteristics of the T1 digital signal format are as follows:

- A T1 frame is 193 bits long—8 bits from each of the 24 time slots (digital service 0s [DS0s]) plus 1 bit for framing. A T1 repeats every 125 microseconds, resulting in 8000 samples per second (8 bits x 24 time slots, + 1 framing bit, x 8000 samples/second = 1.544 Mbps).

- T1 has two major framing and/or format standards:

  – Super Frame (SF), or D4, specifies 12 frames in sequence. The D4 framing pattern used in the ‘F’ position in the figure is 100011011100 and synchronizes within four frames. Because there are 8000 T1 frames transmitted per second, 8000 ‘F’ bits are produced and used for framing.

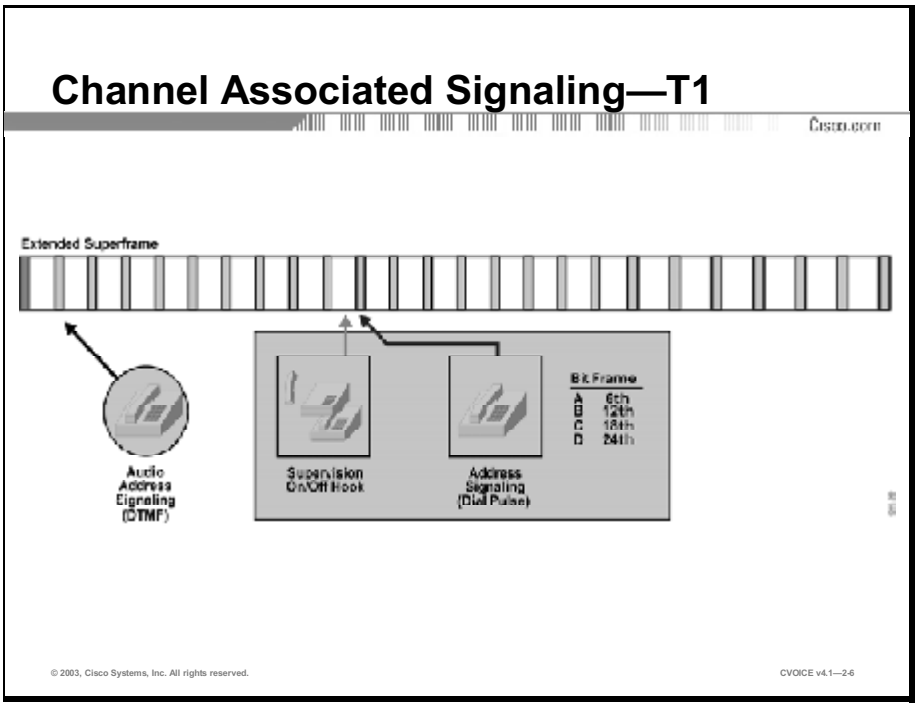
- Extended Superframe (ESF) format was developed as an upgrade to SF and is now dominant in public and private networks. Both types of format retain the basic frame structure of 1 framing bit followed by 192 data bits. However, ESF repurposes the use of the ‘F’ bit. In ESF, of the total 8000 ‘F’ bits used in T1, 2000 are used for framing, 2000 are used for cyclic redunancy check (CRC) (for error checking only), and 4000 are used as an intelligent supervisory channel to control functions end to end (such as loopback and error reporting).



Because each DS0 channel carries 64 kbps, and G.711 is 64 kbps, there is no room to carry signaling. Implemented for voice, the T1 uses every sixth frame to convey signaling information. In every sixth frame, the least significant bit (LSB) for each of the voice channels is used to convey the signaling. Although this implementation detracts from the overall voice quality (because only 7 bits represent a sample for that frame), the impact is not significant. This method is called robbed-bit signaling (RBS). When SF employs this method, the signaling bits are conveyed in both the 6th (called the ‘A’ bit) and 12th (called the ‘B’ bit) frames. For control signaling, A and B bits provide both near- and far-end off-hook indication.

The A and B bits can represent different signaling states or control features (on/off hook, idle, busy, ringing, and addressing). The robbed bit is the least significant bit from an 8-bit word.

ESF also uses RBS in frames 6, 12, 18, and 24, which yields ABCD signaling options, providing additional control and/or signaling information



Because the signaling occurs within each DS0, it is referred to as in band. Also, because the use of these bits is exclusively reserved for signaling each respective voice channel, it is referred to as CAS.

The robbed bits are used to convey ear and mouth (E&M) status or Foreign Exchange Station/Foreign Exchange Office (FXS/FXO) status and provide call supervision for both on hook and off hook.

Example

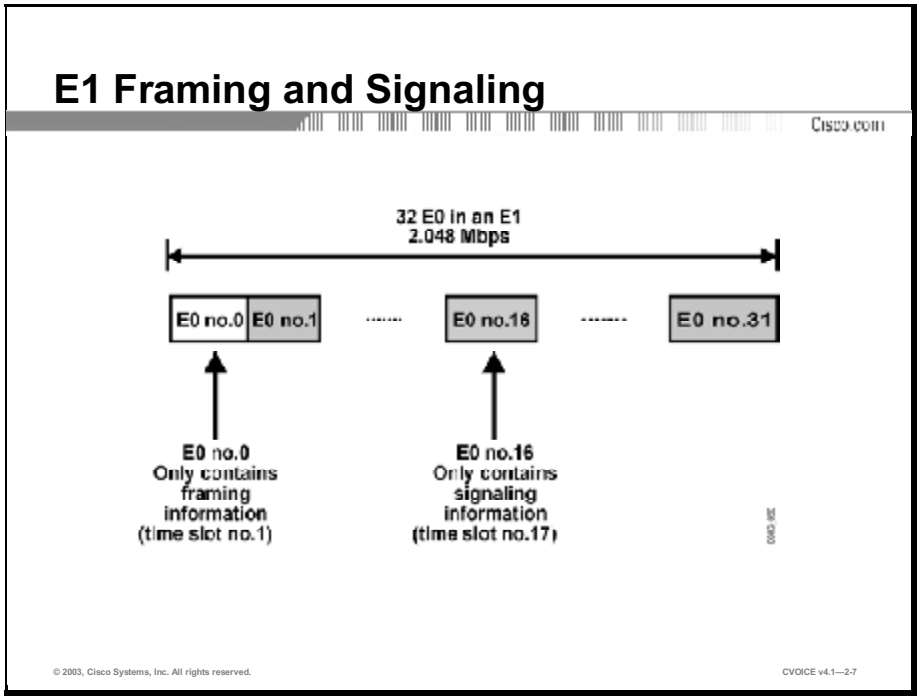
D4 has a 12-frame structure and provides AB bits for signaling.

ESF has a 24-frame structure and provides ABCD bits for signaling.

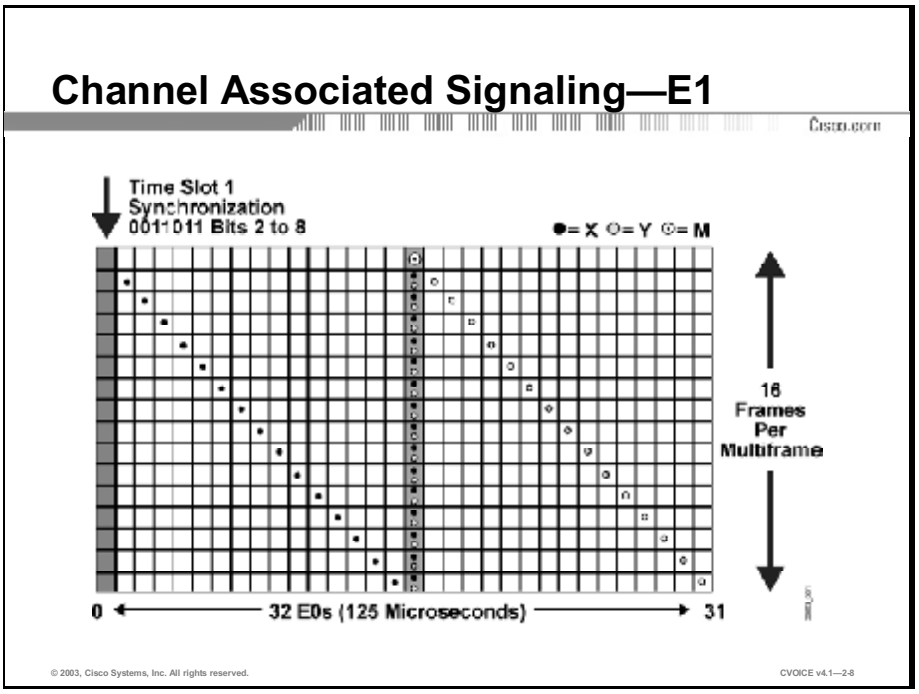
Dual tone multifrequency (DTMF), or tone, can be carried in band in the audio path; however, other supervisory signals must still be carried via CAS.

Channel Associated Signaling Systems: E1

This topic describes CAS and its uses with E1 transmission.



In E1 framing and signaling, 30 of the 32 available channels, or time slots, are used for voice and data. Framing information uses time slot 1, while time slot 17 (E0 16) is used for signaling by all the other time slots. This signaling format is also known as CAS because the use of the bits in the 17th timeslot is exclusively reserved for the purpose of signaling each respective channel. However, this implementation of CAS is considered out of band because the signaling bits are not carried within the context of each respective voice channel, as is the case with T1.



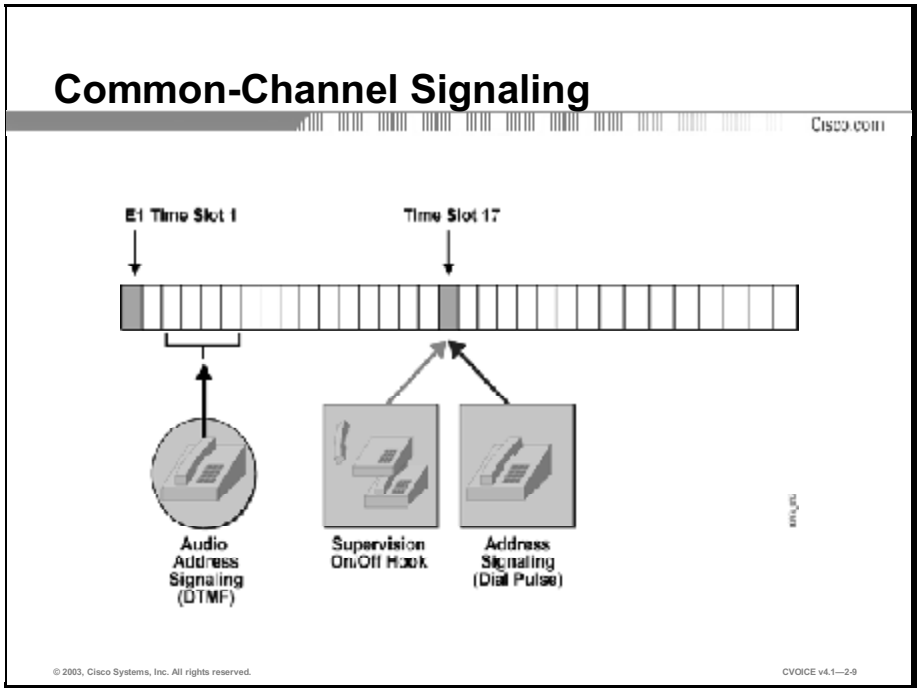
In the E1 frame format, 32 time slots make up a frame. A multiframe consists of 16 E1 frames, as depicted in the figure.

The time slots are numbered 1 though 32. Multiframe time slots are configured as follows:

- Time slot 1 carries only framing information.
- Time slot 17, in the first frame of the 16-frame multiframe, declares the beginning of the multiframe, which is indicated by the ‘M’ symbol in the figure.
- The remaining slot 17s carry signaling information for all the other time slots:
  - Slot 17 of the first frame declares the beginning of a 16-frame multiframe (M).
  - Slot 17 of the second frame carries ABCD for voice slot 2 (X) and ABCD for voice slot 18 (Y).
  - Slot 17 of the third frame carries ABCD for voice slot 3 (X) and ABCD for voice slot 19 (Y).
  - This process continues for all of the remaining frames.

Common Channel Signaling Systems

This topic describes common channel signaling (CCS) systems.



CCS differs from CAS in that all channels use a common channel and protocol for call setup. Using E1 as an example, a signaling protocol, such as the ISDN Q.931, would be deployed in timeslot 17 to exchange call-setup messages with its attached telephony equipment.

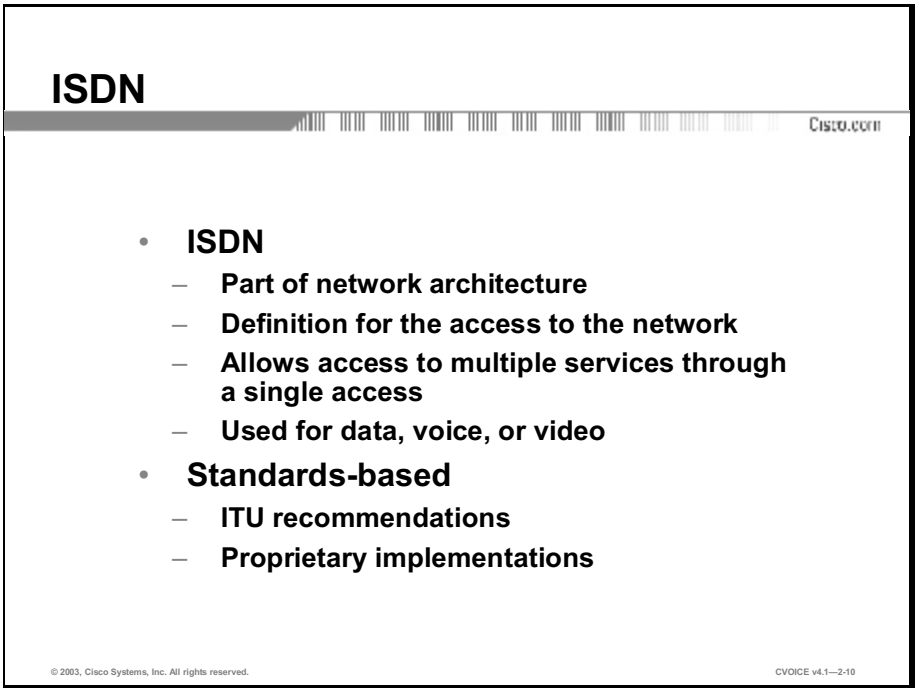
Example

Examples of CCS signaling are as follows:

- **Proprietary implementations:** Some PBX vendors choose to use CCS for T1 and E1and implement a proprietary CCS protocol between their PBXs. In this implementation, Cisco devices are configured for Transparent-Common Channel Signaling (T-CCS) because they do not understand proprietary signaling information.
- **ISDN:** Uses Q.931 in a common channel to signal all other channels
- **Digital Private Network Signaling System (DPNSS):** An open standard developed by British Telecom for implementation by any vendor who chooses to use it. DPNSS also uses a common channel to signal all other channels.
- **Q Signaling (QSIG):** Like ISDN, uses a common channel to signal all other channels.
- **Signaling System 7:** An out-of-band network implemented and maintained by various telephone companies and used for signaling and other supplemental services.

ISDN

This topic describes how to implement ISDN as a signaling system to support voice.



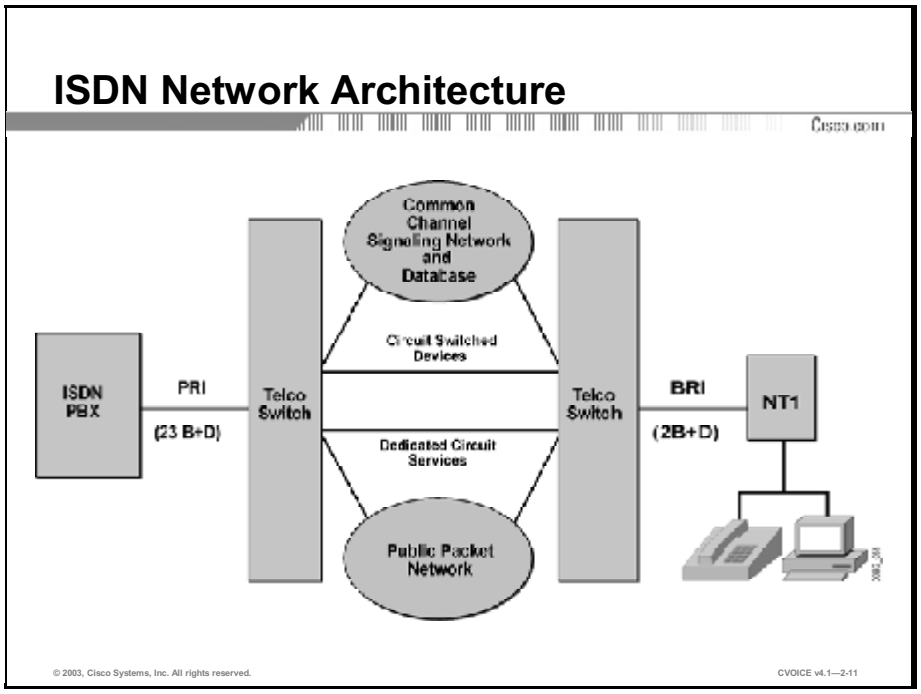
ISDN is an access specification to a network. You may have studied ISDN as an access method for dialup data systems. Because it is a digital system, ISDN makes connections rapidly.

ISDN can be implemented in two different ways: BRI and PRI. BRI features two bearer (B) channels, while PRI supports 23 (for T1) or 30 (for E1) B channels. Each implementation also supports a data (D) channel, used to carry signaling information (CCS).

The following are benefits of using ISDN to convey voice:

- Each B channel is 64 kbps, making it perfect for G.711 pulse code modulation (PCM)
- ISDN has a built-in call-control protocol known as International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Q.931
- ISDN can convey standards-based voice features, such as call forward
- ISDN supports standards-based enhanced dialup capabilities, such as Group IV fax and audio channels

Note ISDN BRI voice is commonly used in Europe; ISDN PRI voice is used worldwide.

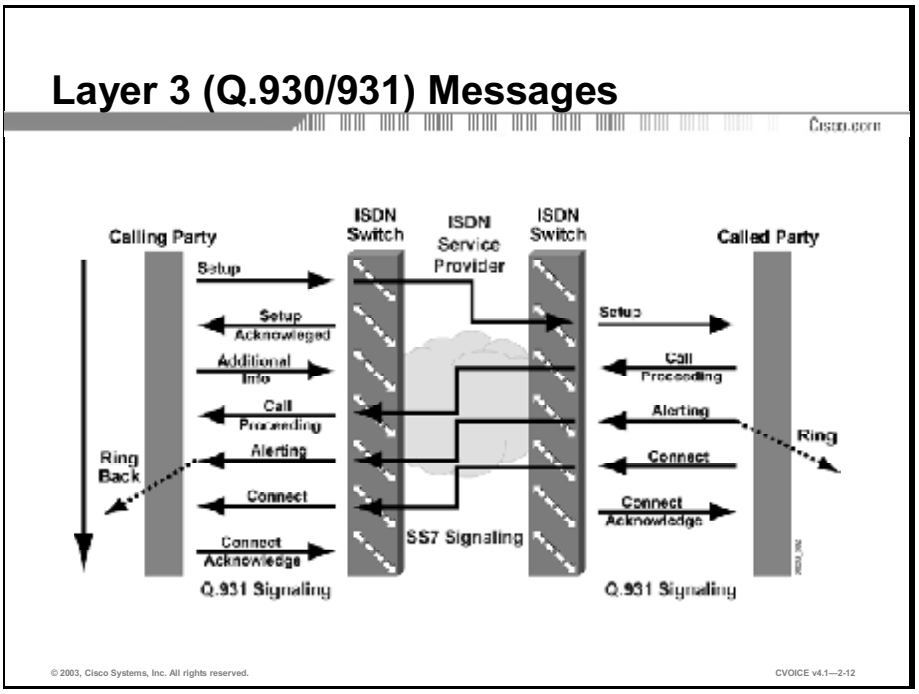


The figure here depicts the architecture of an ISDN network. The B channel carries information, such as voice, data, and video, at 64-kbps DS0.

The D channel carries call signaling between customer premises equipment (CPE) and the network, usually as the Q.931 protocol but sometimes as the QSIG (point of the ISDN model) protocol.

BRI operates using the average local copper pair. It uses two B channels and one signaling channel. It is represented as 2 B+D.

PRI implemented on T1 uses 23 B channels and one signaling channel. It is represented as 23 B+D. PRI implemented on E1 uses 30 B channels and one signaling channel. It is represented as 30 B+D.



Layer 3, Q.931, uses a standard set of messages to communicate. These standard commands cover the following areas:

- **Call establishment:** Initially sets up a call. Messages travel between the user and the network. Call establishment events include: alerting, call proceeding, connect, connect acknowledgment, progress, setup, and setup acknowledgment.

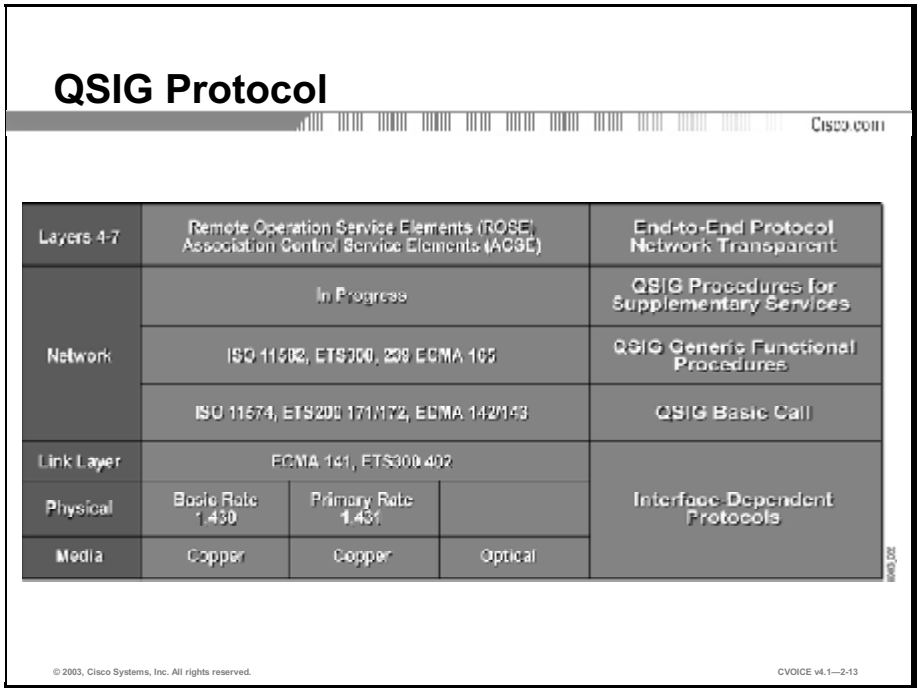
- **Call information phase:** Data sent between the user and the network after the call is established. This allows the user to, for example, suspend and then resume a call. Events in the call information phase include: hold, hold acknowledgment, hold reject, resume, resume acknowledgment, resume reject, retrieve, retrieve acknowledgment, retrieve reject, suspend, suspend acknowledgment, suspend reject, and user information.

- **Call clearing:** Terminates a call. The following events occur in the call-clearing phase: disconnect, release, release complete, restart, and restart acknowledgment.

- **Miscellaneous messages:** Negotiates network features (supplementary services). Miscellaneous services include congestion control, facility, information, notify, register, status, and status inquiry.

Q Signaling

This topic lists the benefits of using QSIG to support voice.



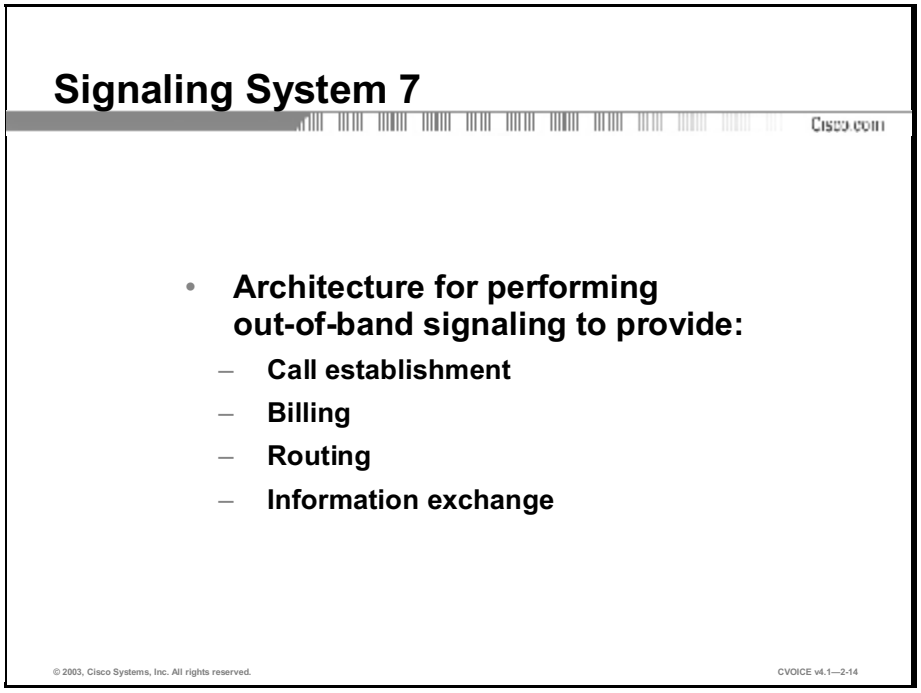
The QSIG protocol, which is based on the ISDN Q.931 standard, provides signaling for private integrated services network exchange (PINX) devices. PINX includes everything from PBXs and multiplexers to Centrex. By using QSIG PRI signaling, a Cisco device can route incoming voice calls from a PINX across a WAN to a peer Cisco device, which can then transport the signaling and voice packets to a second PINX. QSIG is implemented on PRI interfaces only. ISDN PRI QSIG voice-signaling provides the following benefits:

- Connect the Cisco device with digital PBXs that use the QSIG form of CCS
- Provides transparent support for supplementary PBX services so that proprietary PBX features are not lost when connecting PBXs to Cisco networks
- Provides QSIG support based on widely used ISDN Q.931 standards and the European Telecommunication Standards Institute (ETSI) implementation standards. These include:
  - **European Computer Manufacturers Association (ECMA) 143:** Private Telecommunication Network (PTN) Interexchange Signaling Protocol Circuit Mode Basic Services (this specification covers QSIG basic call services)

- **ECMA 142:** Specification, Functional Model and Information Flows for Control Aspects of Circuit Mode Basic Services in PTNs
- **ECMA 141:** PTN Interexchange Signaling Data Link Layer Protocol
- **ECMA 165:** Generic Functional Protocol for the Support of Supplementary Services

Signaling System 7

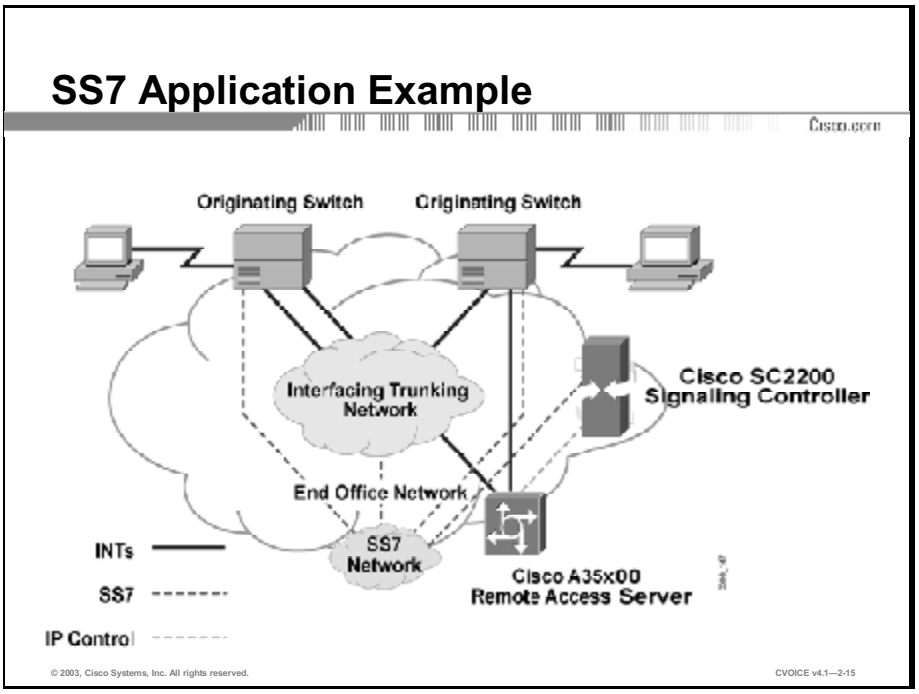
This topic lists the primary functions and benefits of SS7.



The ITU-T (formerly the CCITT) developed SS7 in 1981. The primary functions and benefits of SS7 are as follows:

- Fast call setup by high-speed circuit-switched connections
- PBX transaction capabilities (that is, call forwarding, call waiting, call screening, and call transfer) extended to the entire network
- Dedicated control channel for all signaling functions
- Each associated trunk group needs only one set of signaling facilities
- Information, such as address digits, can be transferred directly between control elements
- No chance of mutual interference between voice and control channel because SS7 is out-of-band signaling
- Because the control channel is not accessible by the user, possible fraudulent use of the network is avoided
- Connections involving multiple switching offices can be set up more quickly

Note The channel used for CCS does not need to be associated with any particular trunk group.

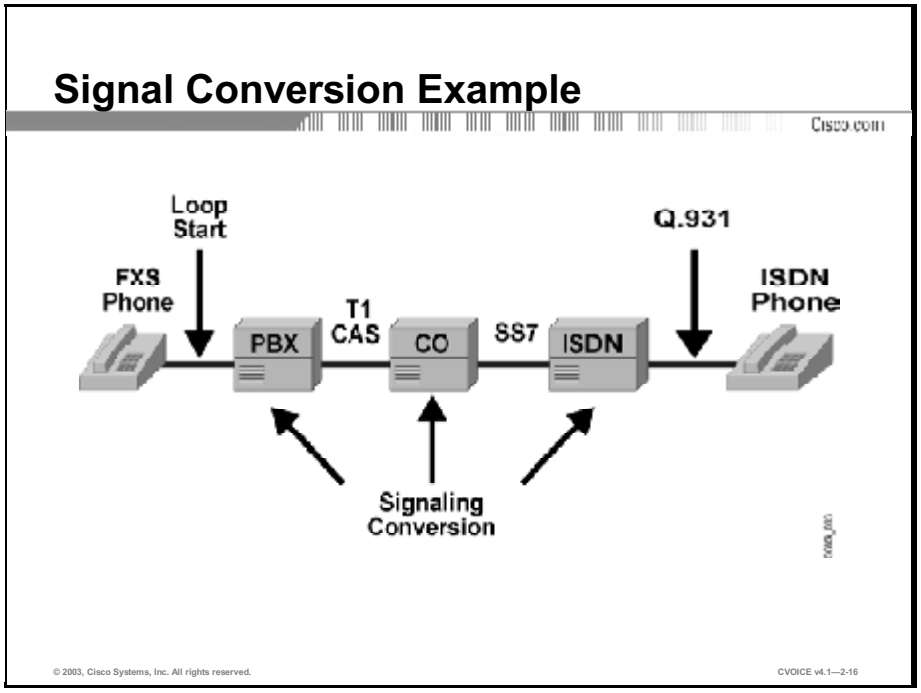


The figure here depicts an implementation of SS7. As a function of customer networks, SS7 can be implemented as a CSS across a telephony network enterprise. Using Cisco equipment, service providers can implement SS7 on their networks. Cisco has developed several solutions that support offloading IP traffic from public networks and support the direct connection of network access servers to the public switched telephone network (PSTN) using SS7 links. These solutions utilize the Cisco PGW2200, BTS10200, and Cisco AS5x00, giving service providers a proven and cost-efficient SS7 solution for connecting dial-access servers and voice gateways to the PSTN.

The Cisco AS5x00 family provides carrier-class, high-density connectivity for Voice over IP (VoIP) and dial subscribers. The product set supports a wide range of IP services (including voice) and enables carriers and Internet service providers (ISPs) to cost effectively support increased subscriber services and an increasing subscriber base.

Signaling Systems Interworking

This topic describes how different signaling systems interoperate on the same voice system.



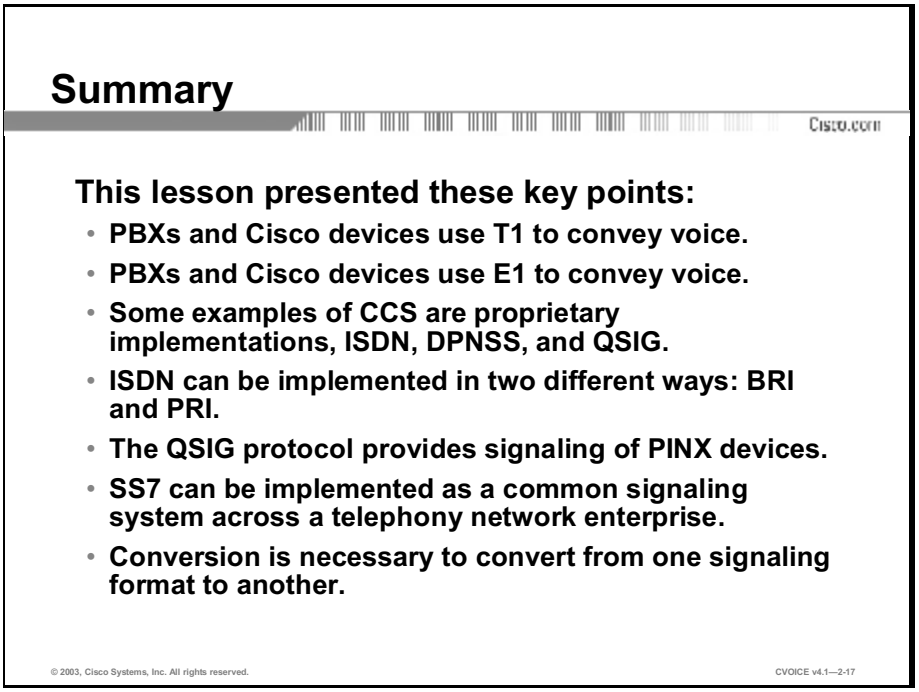
In some implementations, it is necessary to convert from one signaling format to another. Conversion is necessary to allow different systems to signal each other. The figure illustrates this example.

Telephone A is using FXS loop-start signaling to connect to the PBX. The user dials 9 for an outside line, which carries the call on the T1 by using CAS. After the call reaches the central office (CO), it travels via an SS7 signaled circuit to an ISDN switch. The call is then conveyed via Q.931 to the ISDN telephone at the called party location.

Other conversion applications exist in voice telephony. The telephony equipment must have the capability to perform these conversions.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Signaling Systems
- Assessment (Complex Lab): Refer to Lab 2-1, contained in Laboratory Exercises in Additional Resources section E.
- FAX and Modem over Voice over IP lesson

References

For additional information, refer to these resources:

- "Voice Network Signaling and Control" http://www.cisco.com/warp/public/788/signalling/net_signal_control.html

Quiz: Signaling Systems

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- State the uses and types of channel associated signaling systems used for T1
- State the uses and types of channel associated signaling systems used for E1
- State the uses and types of common channel signaling systems
- Name the benefits of using ISDN to convey voice
- Name the benefits of using Q Signaling to convey voice
- Name the functions of Signaling System 7 and its benefits
- Describe how separate signaling systems can be interfaced

Instructions

Answer these questions.

Q1) In a T1 using CAS, what is the F bit in the ESF used for?

A) framing

B) CRC

C) supervisory channel

D) all of the above

Q2) In CAS, what type of control information is provided by the A and B bits in SF?

A) near- and far-end off-hook

B) idle

C) busy

D) ringing

E) addressing

F) all of the above

Q3) How many timeslots are there in an E1 frame using CAS?

A) 16

B) 24

C) 30

D) 32

Q4) In an E1 frame using CAS, which bits are reserved for signaling?

A) all the bits in time slot 16

B) all the bits in time slot 17

C) the first bit in time slot 17

D) the least significant bit in time slot 1

Q5) Which signaling method is NOT an example of CCS?

A) DPNSS

B) ISDN

C) QSIG

D) RBS

E) SS7

Q6) If vendors use a proprietary CCS protocol between their PBXs, how must Cisco devices be configured?

A) CCS

B) CCSS7

C) SS7

D) T-CCS

Q7) What type of information is carried in the D channel of ISDN?

A) voice

B) video

C) data

D) signaling

Q8) How many B channels and signal channels are implemented on a PRI T1?

A) 1 B channel and 1 signaling channel

B) 2 B channels and 1 signaling channel

C) 23 B channels and 1 signaling channel

D) 30 B channels and 1 signaling channel

Q9) What type of interfaces support QSIG?

A) BRI

B) PRI

C) T1

D) E1

Q10) Which ISDN standard is QSIG based on?

A) Q.2931

B) Q.931

C) Q.920

D) Q.93B

Q11) Which function is performed by SS7?

A) call establishment

B) billing

C) routing

D) information exchange

E) all of the above

Q12) SS7 was developed by _____.

A) IETF

B) ISO

C) ITU

D) Cisco

Q13) Why is signal conversion necessary?

A) To allow different systems to signal each other

B) To convert G.711 to G.729

C) To convert voice to data

D) To encode and compress voice

Q14) Which signaling method would be required between a CO and an ISDN switch?

A) loop start

B) T1 CAS

C) SS7

D) E1 CAS

E) RBS

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Fax and Modem over Voice over IP

Overview

This lesson describes the implementation of fax and modem traffic over a Voice over IP (VoIP) network. It explores both the Cisco Systems and the standard implementations of fax and various methods used to transport modem traffic over VoIP.

Importance

This lesson provides information about fax and modem traffic over VoIP for purposes of implementation. This lesson is necessary to educate the student in the methods used to implement a VoIP network.

Objectives

Upon completing this lesson, you will be able to:

- State the method used for conveying fax using Cisco fax relay
- State the method used for conveying fax using T.38 fax relay
- State the applications for and the method used to convey fax using T.37 store-and-forward fax
- Describe how fax passthrough operates in a Voice over IP network
- Describe how modem passthrough operates in a Voice over IP network
- Describe how modem relay operates in a Voice over IP network

Learner Skills and Knowledge

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

- Knowledge of basic VoIP
- Familiarity with fax technology
- Familiarity with modem technology
- Familiarity with basic digital signal processor (DSP) use

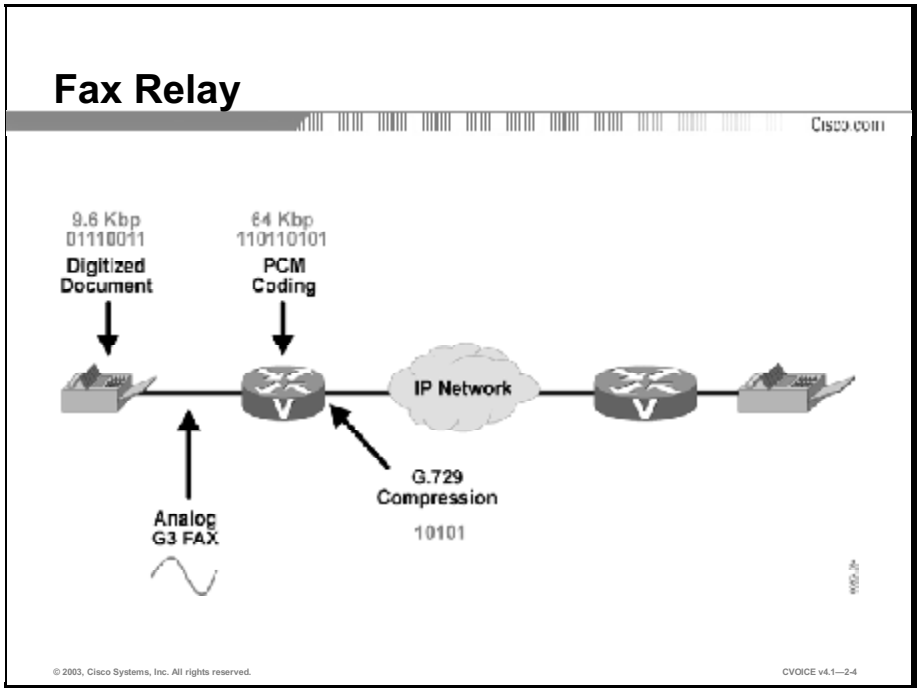
Outline

This lesson includes these topics:

- Overview
- Cisco Fax Relay
- T.38 Fax Relay
- T.37 Fax Store and Forward
- Fax Passthrough
- Modem Passthrough
- Modem Relay
- Summary
- Assessment (Quiz): Fax and Modem over Voice over IP
- Assessment (Complex Lab): Lab Exercise 2-1

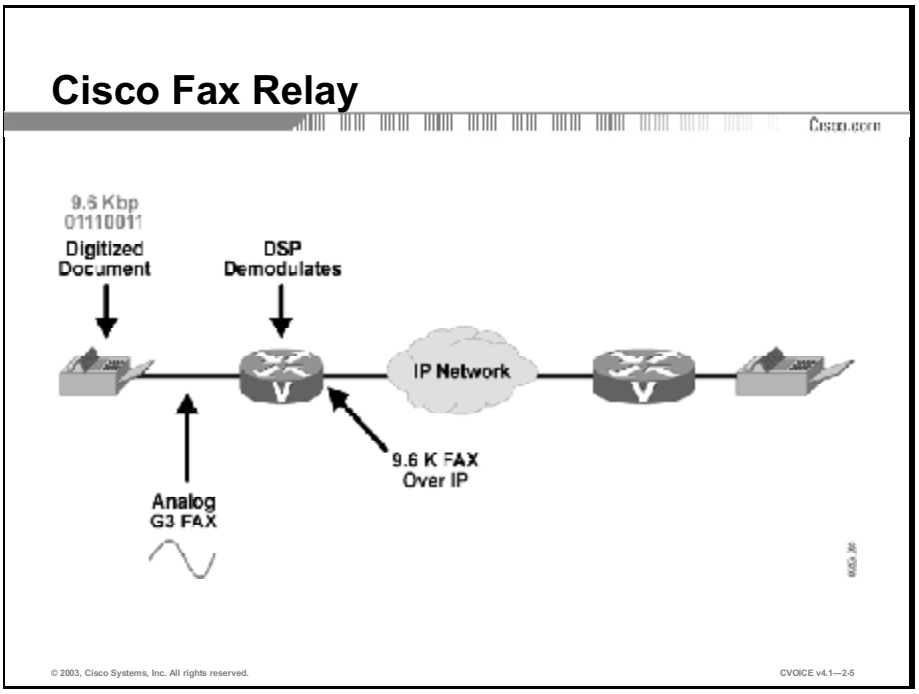
Cisco Fax Relay

This topic describes how the Cisco fax relay operates in a VoIP network.



The figure depicts a VoIP network set up for fax relay. Initially, fax calls are digitized representations of the contents on paper. The digitized bit stream is then converted to analog for transmission over voice circuits. If Cisco equipment treated fax calls like voice calls, the analog waveform would then be converted to G.711 pulse code modulation (PCM) at 64 kbps and subsequently compressed before transmission across the VoIP network.

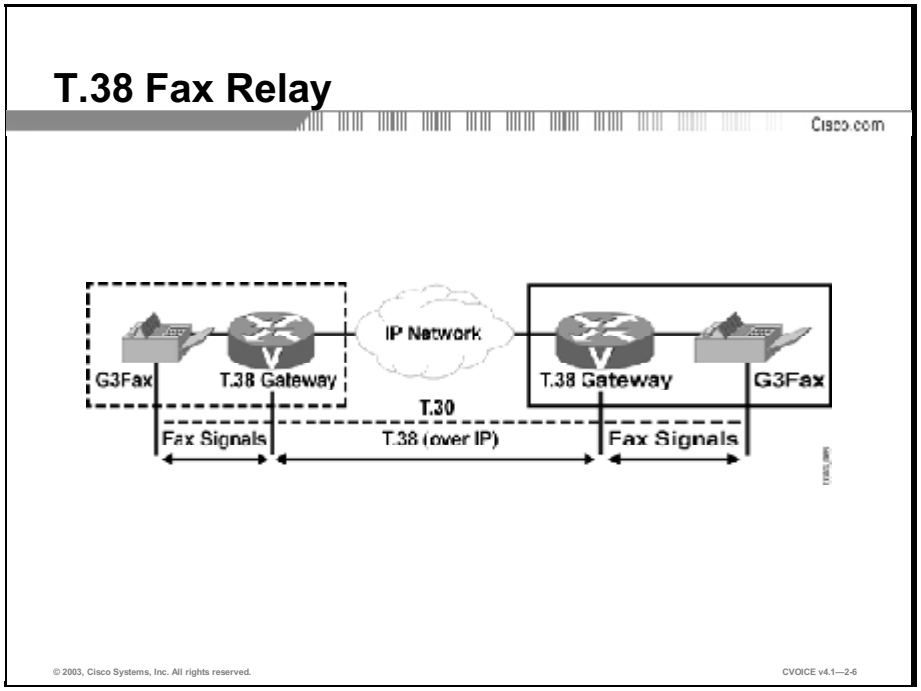
This approach is impractical because there are too many conversions and because the coding and compression schemes are designed to convey human speech, not fax modem tones.



The figure depicts Cisco fax relay operating in a VoIP network. Using Cisco fax relay, the DSP chip first sets up the call as an end-to-end voice call. The DSP then recognizes the tones as those coming from a fax machine. The local DSP assumes the role of a fax modem, converting the analog data back to the original digitized bit stream. The fax modem is downshifted in speed to 9.6 kbps to save bandwidth over the IP path. The bit stream is then packaged in VoIP packets and identified as a fax. The remote DSP assumes a similar role and converts the bit stream to analog for reception by the remote fax machine.

T.38 Fax Relay

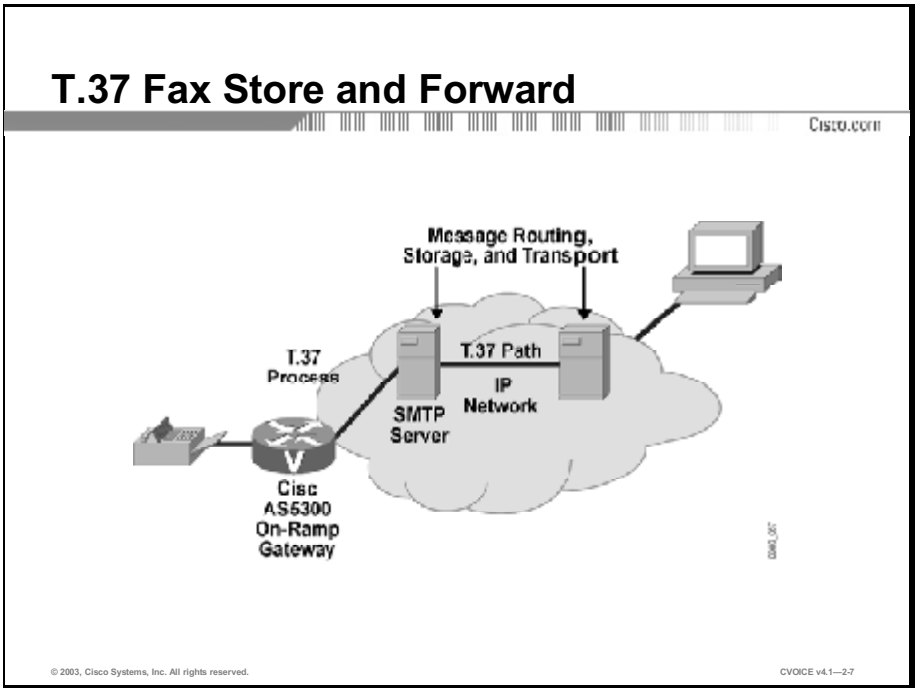
This topic describes how International Telecommunication Union (ITU) standard T.38 fax relay operates in a VoIP network.



The T.38 approach is similar to the Cisco approach, but represents the industry standard. The figure depicts T.38 fax relay. In this approach, a T.38 gateway is required at both ends. A Cisco voice-enabled router can be configured as a T.38 gateway, and the transmission methodology is similar to the Cisco fax relay method. However, with T.38 it is possible to deliver documents to virtual fax machines, such as PCs and servers, that are configured with software that is compatible with T.38 fax.

T.37 Fax Store and Forward

This topic describes how ITU standard T.37 store-and-forward fax operates in a VoIP network.



The figure depicts the T.37 fax store-and-forward method. The T.37 standard is a way of delivering faxed documents as e-mail attachments. T.37 works by scanning a document, converting that document to tagged image file format (TIFF), and sending it to an e-mail address as an attachment using Simple Mail Transfer Protocol (SMTP). Cisco implements T.37 fax store and forward by using special gateways that are configured as on-ramps (transmitters of fax) or off-ramps (receivers of fax).

When configured on an on-ramp gateway, store-and-forward fax provides a way to transform standard fax messages by entering a packet network into e-mail messages and TIFF attachments that travel to PCs on the network. When configured on an off-ramp gateway, e-mail with TIFF attachments transform into standard fax messages. These messages travel out of the packet network to standard group three fax devices on the public switched telephone network (PSTN). When configured on both the on-ramp and off-ramp gateways of a network, store-and-forward fax allows temporary storage in the packet network for standard fax messages that cannot be delivered immediately.

Example

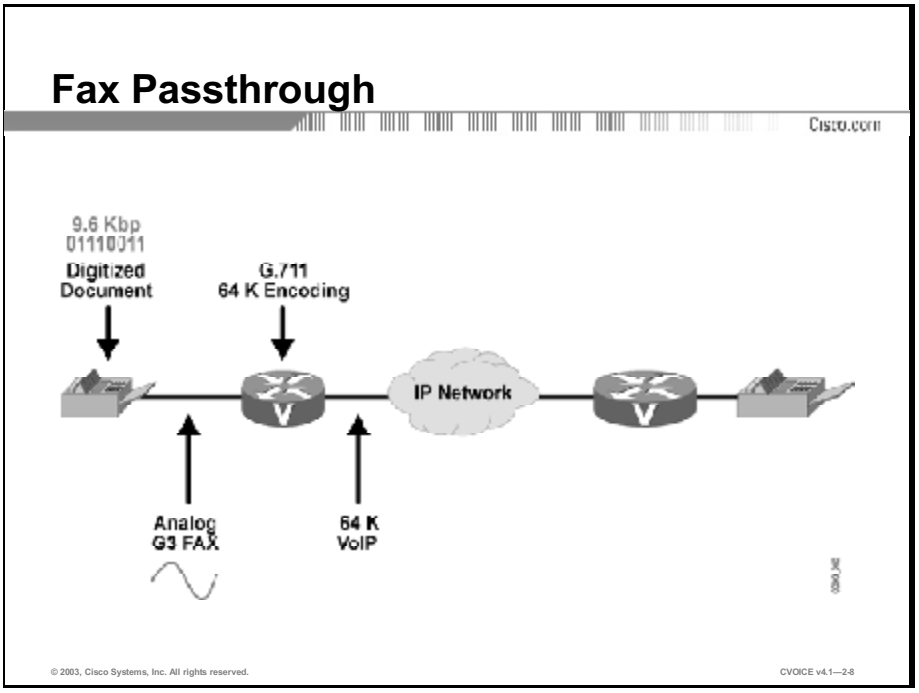
Store-and-forward fax uses two different interactive voice response (IVR) applications for on-ramp and off-ramp functionality. The applications are implemented in two Tool Command Language (TCL) scripts that you can download from www.cisco.com.

SMTP facilitates the basic functionality of store-and-forward fax, with additional functionality that provides confirmation of delivery using existing SMTP mechanisms such as Extended Simple Mail Transfer Protocol (ESMTP). Store-and-forward fax requires that you configure gateway dial peers and the following types of parameters:

- **IVR application parameters and IVR security and accounting parameters:** Load the applications on the router and enable accounting and authorization for the application
- **Fax parameters:** Specify the cover sheet and header information for faxes that are generated in the packet network
- **Message Transfer Agent (MTA) parameters:** Define delivery parameters for the e-mail messages that accompany fax TIFF images
- **Message disposition notification (MDN) parameters:** Specify the generation of messages to notify e-mail originators when their fax e-mail messages are delivered
- **Delivery status notification (DSN) parameters:** Instruct the SMTP server to send messages to e-mail originators to inform them of the status of their e-mail messages
- **Gateway security and accounting parameters:** Define authentication, authorization, and accounting (AAA) for faxes that enter or exit the packet network

Fax Passthrough

This topic describes how fax passthrough operates in a VoIP network.



This figure depicts fax passthrough in a VoIP network. Fax passthrough occurs when incoming T.30 fax data is not demodulated or compressed for its transit through the packet network. The two fax machines communicate directly to each other over a transparent IP connection.

When a gateway detects a fax tone, it switches the call to a high-bandwidth coder-decoder (codec). The fax traffic, still in PCM form, travels in band over VoIP using G.711 with no voice activity detection (VAD). This method of transporting fax traffic takes a constant 64-kbps (payload) stream end to end for the duration of the call. It is very sensitive to packet loss, jitter, and latency in the IP network, although packet redundancy can be used to mitigate the effects of packet loss.

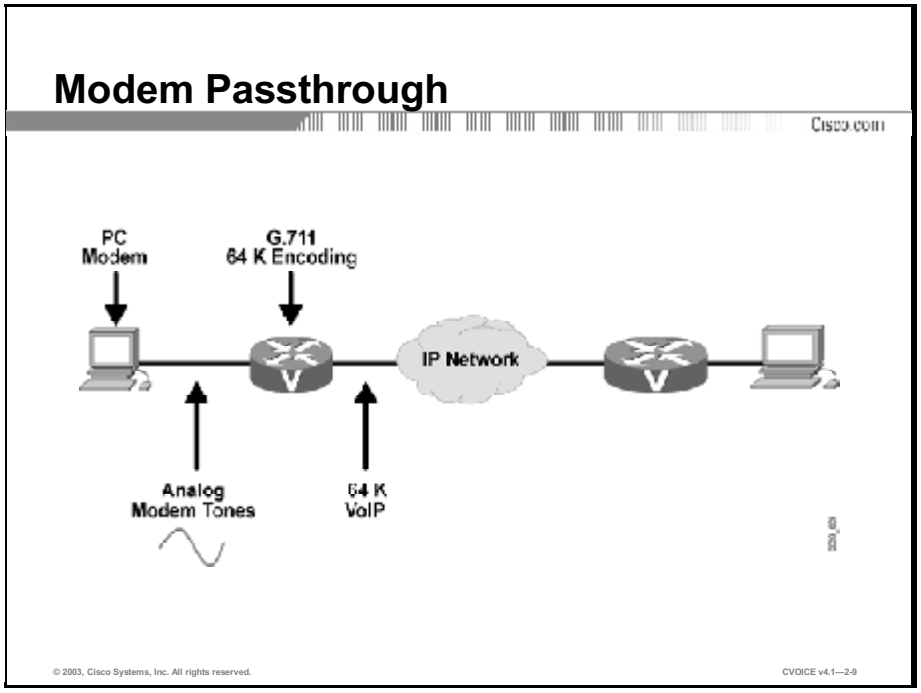
Fax passthrough is supported under the following call-control protocols:

- H.323
- Session initiation protocol (SIP)
- Media Gateway Control Protocol (MGCP)

Note	Echo cancellation is enabled and preferred for passthrough using Cisco IOS® Release 12.0(3) T and later. Earlier versions of Cisco IOS required that you disable echo cancellation.

Modem Passthrough

This topic describes how modem passthrough operates in a VoIP network.



The figure depicts modem passthrough in a VoIP network. Modem passthrough is similar to fax passthrough, except that there is a computer modem at each end of the connection. The two modems communicate directly with each other over a transparent IP connection.

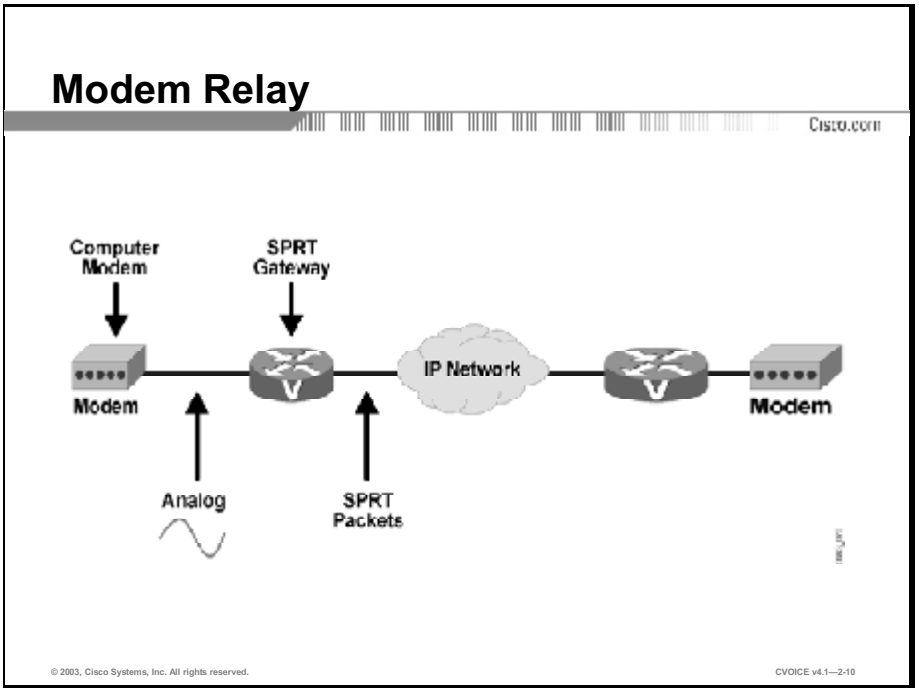
When a gateway detects a modem tone, it switches the call to a high-bandwidth codec. The modem traffic, still in PCM form, travels in band over VoIP using G.711 with no VAD. This method of transporting modem traffic takes a constant 64-kbps (payload) stream end to end for the duration of the call. It is highly sensitive to packet loss, jitter, and latency in the IP network, although packet redundancy can be used to mitigate the effects of packet loss.

The following call control protocols support modem passthrough:

- H.323
- SIP
- MGCP

Modem Relay

This topic describes how modem relay operates in a VoIP network.



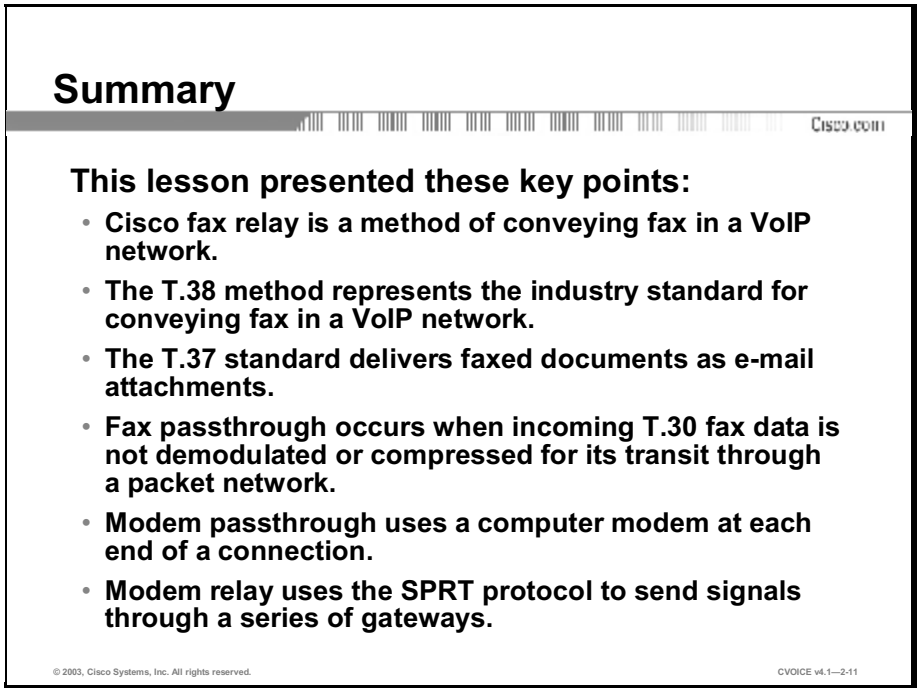
The figure depicts modem relay in a VoIP network. When using modem relay, computer modem signals are demodulated at one gateway, converted to digital form, and carried in Simple Packet Relay Transport (SPRT) protocol packets to the other gateway. When it reaches the other gateway, the modem signal is recreated and remodulated and then passed to the receiving computer modem. SPRT is a protocol running over User Datagram Protocol (UDP). At the end of the modem, the voice ports revert to the previous configuration, and the DSPs switch back to the original voice codec. This method uses less bandwidth (RTP is not required) and is much less sensitive to jitter and clocking mismatches than modem passthrough.

The following call-control protocols support modem relay:

- H.323
- SIP
- MGCP

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Fax and Modem over Voice over IP
- Assessment (Complex Lab): Refer to Lab 2-1, contained in Laboratory Exercises in Additional Resources section E.
- Configuring Voice Interfaces module

References

For additional information, refer to these resources:

- "Cisco Fax Services over IP" http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/index.htm

Quiz: Fax and Modem over Voice over IP

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests you knowledge on how to:

- State the method used for conveying fax using Cisco fax relay
- State the method used for conveying fax using T.38 fax relay
- State the applications for and the method used to convey fax using T.37 store-and-forward fax
- Describe how fax passthrough operates in a Voice over IP network
- Describe how modem passthrough operates in a Voice over IP network
- Describe how modem relay operates in a Voice over IP network

Instructions

Answer these questions:

Q1) Which device acts as a fax modem in Cisco fax relay?

A) the DSP

B) the gateway

C) the modem

D) the gatekeeper

Q2) What speed does the fax modem operate at in Cisco fax relay?

A) 64 kbps

B) 52 kbps

C) 16 kbps

D) 9.6 kbps

Q3) Which Cisco device or application can be configured as a T.38 gateway?

A) Cisco IP Phone

B) Cisco call-processing agents

C) Cisco carrier-class call agents

D) Cisco voice-enabled routers

Q4) What is the advantage of using T.38 as compared to Cisco proprietary fax relay?

A) T.38 has a faster transmission rate.

B) T.38 allows delivery of documents to virtual fax machines.

C) T.38 uses a more efficient transmission methodology.

D) All of the above.

Q5) How can you provide temporary storage in a packet network for fax messages that need to be delivered?

A) Configure a fax relay buffer on the on-ramp gateways.

B) Configure T.37 store-and-forward fax relay on the on-ramp gateways.

C) Configure T.37 store-and-forward fax relay on the off-ramp gateways.

D) Configure T.37 store-and-forward fax relay on both the on-ramp and off-ramp gateways.

Q6) In T.37 store-and-forward fax relay, which parameters must be configured to instruct the SMTP server to notify e-mail originators of the status of their messages?

A) DSN parameters

B) fax parameters

C) MDN parameters

D) MTA parameters

Q7) Which call-control protocol does not support fax passthrough?

A) H.323

B) SIP

C) MGCP

D) SGCP

Q8) Which feature is enabled for fax passthrough using Cisco IOS Release 12.0(3) T and later?

A) echo cancellation

B) echo suppression

C) VAD

D) PCM

Q9) What is the advantage of using modem relay as compared to modem passthrough?

A) Modem relay requires less bandwidth.

B) Modem relay is supported by more call-control protocols.

C) Modem relay provides more interoperability.

D) Modem relay uses compression mechanisms.

Q10) Which protocol is used to carry modem signals across the network using Modem Relay?

A) SMTP

B) SPRT

C) MGCP

D) RTP

Q11) How does modem passthrough differ from fax passthrough?

A) VAD is enabled.

B) G.711 is not used.

C) There is a computer modem at each end.

D) 64-kbps bandwidth is required.

Q12) How can you reduce the effects of packet loss in modem passthrough?

A) by introducing packet redundancy

B) by increasing bandwidth

C) by reducing latency

D) by using dedicated lines

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

3

Configuring Voice Interfaces

Overview

In this module you will learn basic configuration of analog and digital voice ports. You will also learn how to fine-tune voice ports with port-specific configurations.

Upon completing this module, you will be able to:

- 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, given the requirements for international implementation

Outline

The module contains these lessons:

- Voice Port Configuration
- Adjusting Voice Quality

Voice Port Configuration

Overview

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

Importance

Connecting voice devices to a network infrastructure requires an in-depth understanding of 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:

- Provide examples of seven types of voice port applications
- Set the configuration parameters for Foreign Exchange Station voice ports
- Set the configuration parameters for Foreign Exchange Office voice ports
- Set the configuration parameters for recEive and transMit 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 Transparent Common-Channel Signaling in a Voice over IP environment.
- Use the **show**, **debug**, and **test** commands to monitor and troubleshoot voice ports

Learner Skills and Knowledge

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

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

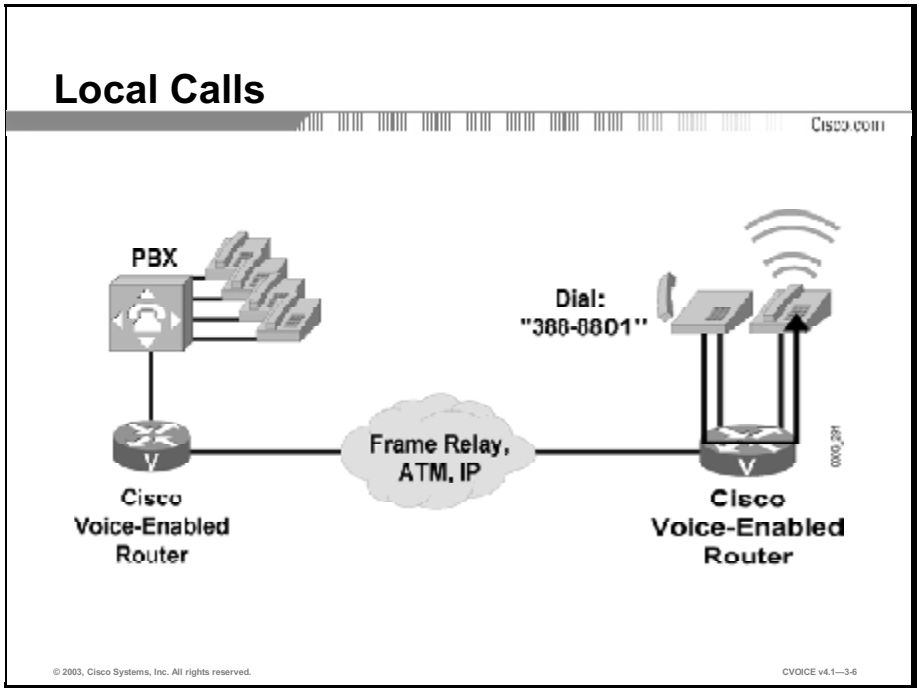
Outline

This lesson includes these topics:

- Overview
- Voice Port Applications
- Foreign Exchange Station Ports
- Foreign Exchange Office Ports
- Ear and Mouth Ports
- Timers and Timing
- Digital Voice Ports
- ISDN
- Common Channel Signaling Options
- Monitoring and Troubleshooting
- Summary
- Assessment (Quiz): Voice Port Configuration
- Assessment (Complex Lab): Lab Exercise 3-1

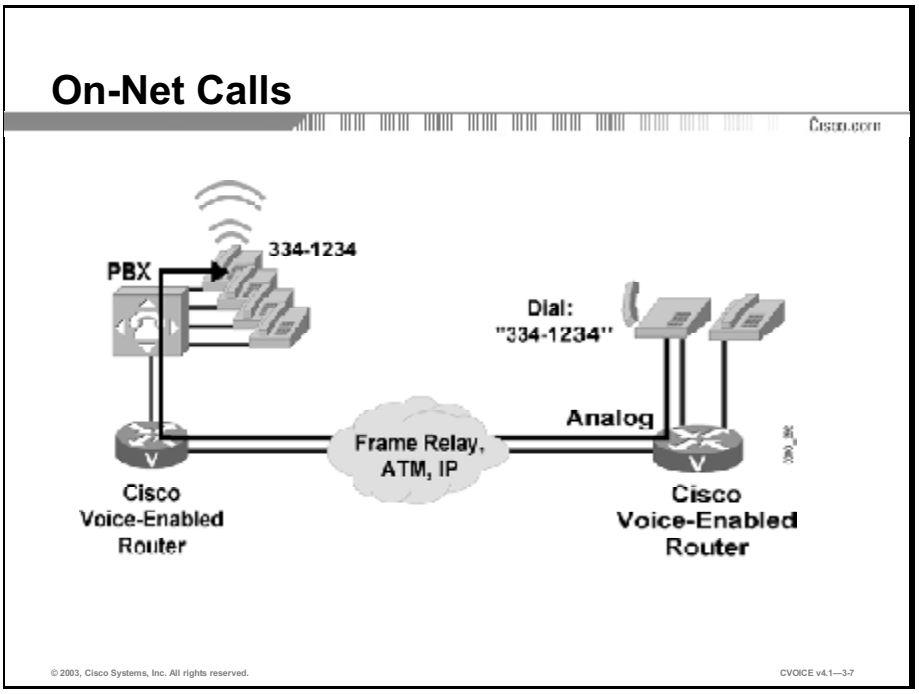
Voice Port Applications

This topic identifies the different types of voice port applications within the network.

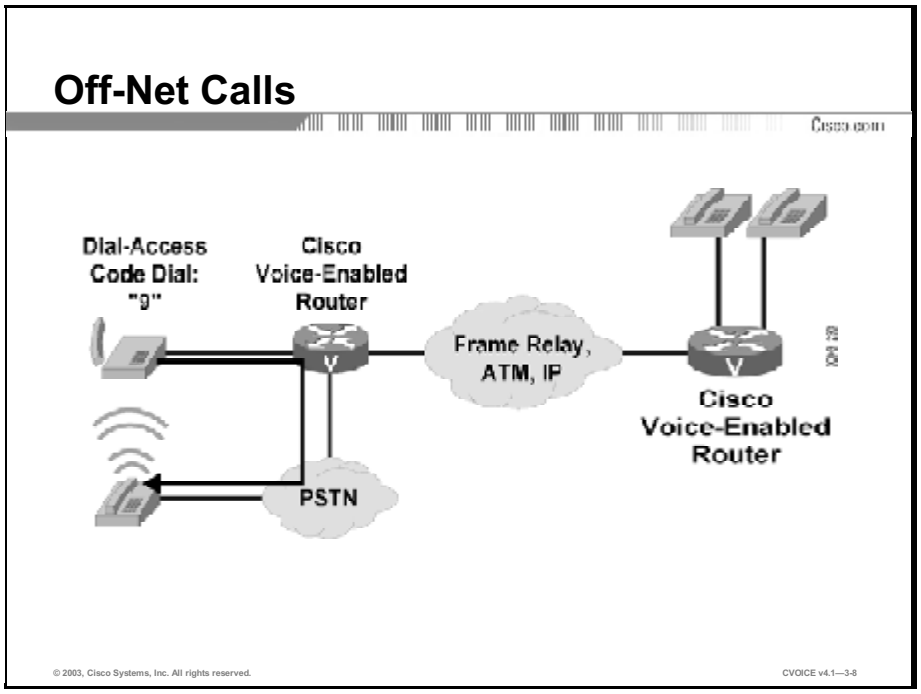


Different types of applications require specific types of ports. In many instances, the type of port is dependent on the voice device that is connected to the network. The following types of calls describe the common applications and port usage.

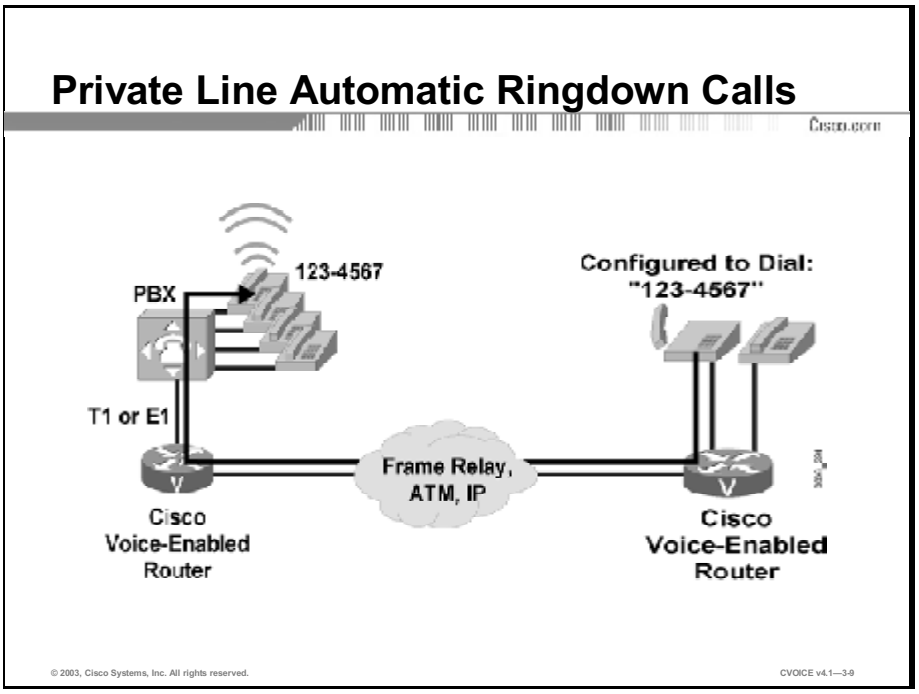
Local calls occur between two telephones connected to one Cisco voice-enabled router. This type of call is handled entirely by the router and does not travel over an external network. Both telephones are directly connected to Foreign Exchange Station (FXS) ports on the router.



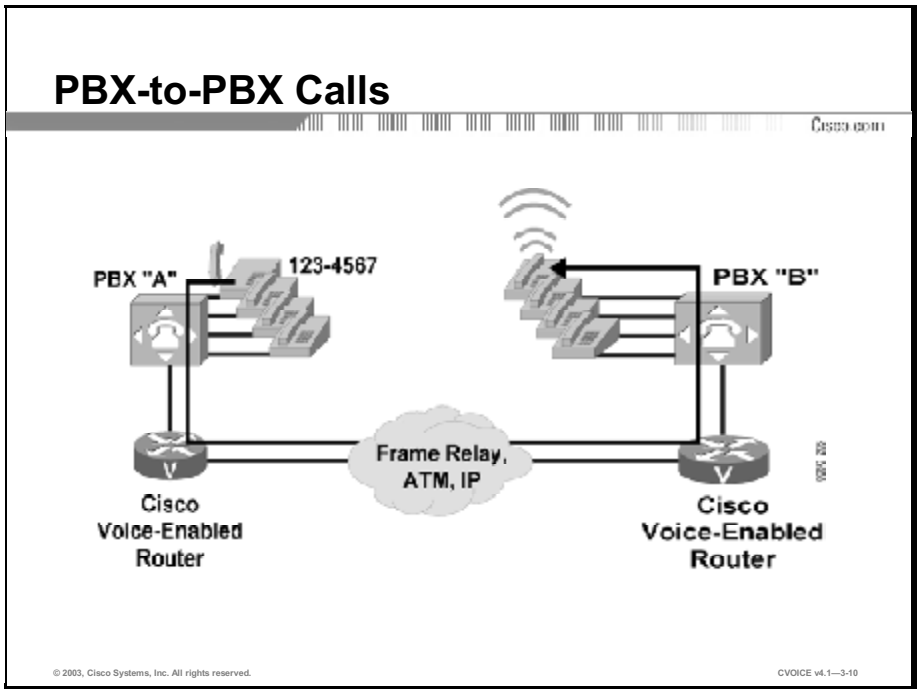
On-net calls occur between two telephones on the same data network. The calls can be routed through one or more Cisco voice-enabled routers, but the calls remain on the same data network. The edge telephones attach to the network through direct connections and FXS ports, or through a PBX, which typically 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 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.



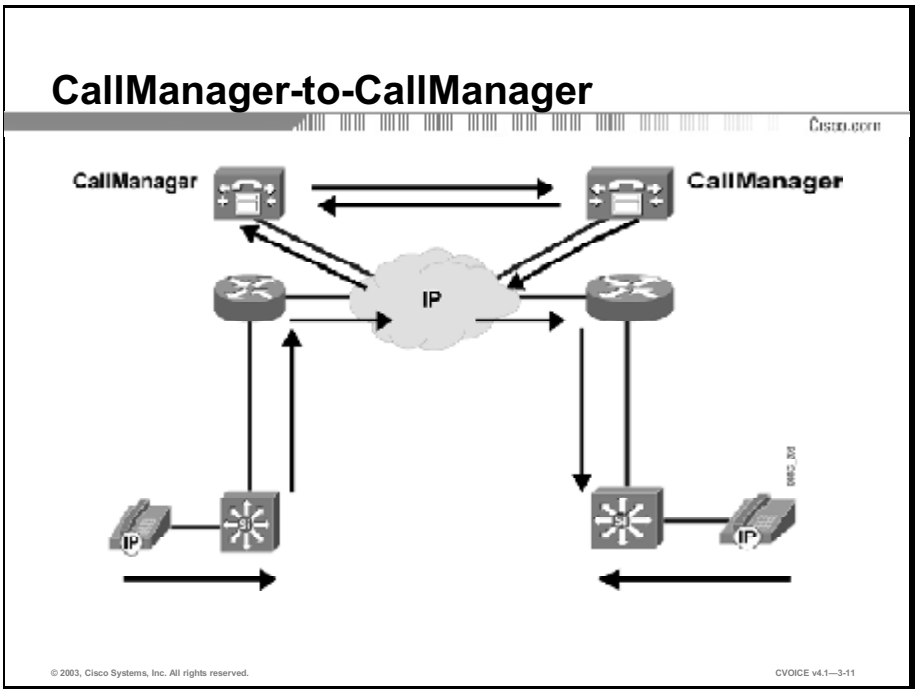
Off-net calls occur when, to gain access to the PSTN, the user dials an access code, such as **9**, from a telephone that is directly connected to a Cisco voice-enabled router or PBX. The connection to the PSTN is a single analog connection via a Foreign Exchange Office (FXO) port or a digital T1 or E1 connection.



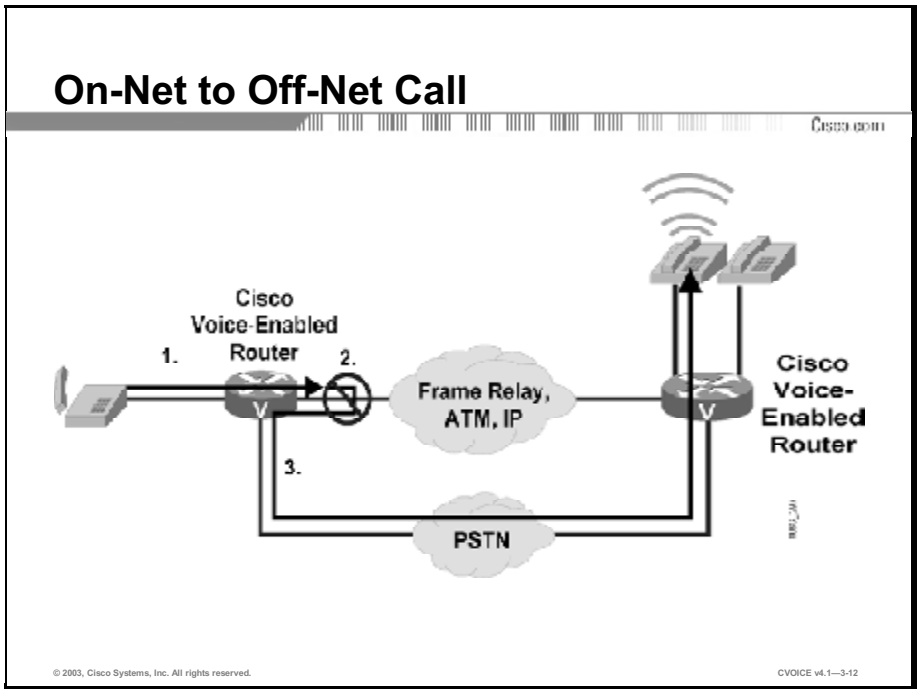
Private line, automatic ringdown (PLAR) calls automatically connect a telephone to a second telephone when the first telephone goes off hook. When this connection occurs, the user does not get a dial tone because the voice-enabled port that the telephone is connected to is preconfigured with a specific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



A PBX-to-PBX call originates at a PBX at one site and terminates at a PBX at another site while using the network as the transport between the two locations. Many business environments connect sites 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, although PBX connections can also be analog.



As part of an overall migration strategy, a business may replace PBXs with a Cisco CallManager infrastructure. This infrastructure includes IP telephones that plug directly into the IP network. Cisco CallManager performs the same call-routing functions formerly provided by the PBX. When an IP phone uses Cisco CallManager to place a call, Cisco CallManager—based on its configuration—assesses 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. Although the call stays on the IP network, it may be sent between zones. Every Cisco CallManager is part of a zone. A zone is a collection of devices that are under a common administration, usually a Cisco CallManager or gatekeeper.



When planning a resilient call-routing strategy, it may be necessary 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 to the PSTN. On-net to off-net call-switching functionality may be necessary when a network link is down, or if a network becomes overloaded and unable to handle all calls presented.

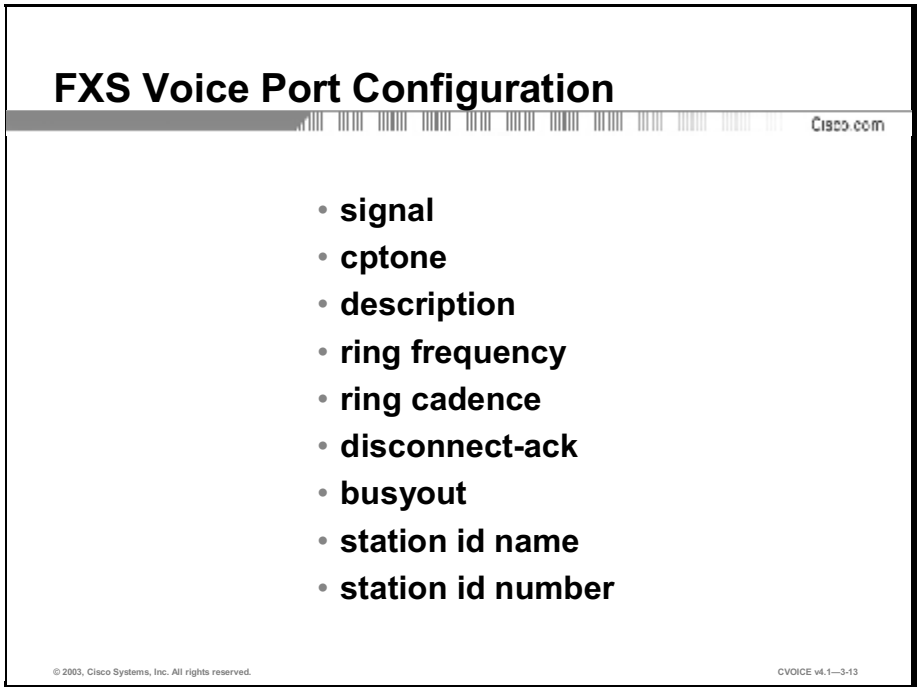
Examples

The table shows examples of each type of call.

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 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 prespecified 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 IP telephones. The call setup is handled by the Cisco CallManagers at both locations. After the call is set up, the IP telephones generate IP packets carrying 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.

Foreign Exchange Station Ports

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



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

For example, consider the scenario of an international company with offices in the United States and England. The PSTN of each country provides signaling that is standard for that country. In the United States, the PSTN provides a dial tone that is different from the tone in England. When the telephone rings to signal an incoming call, the ring is different in the United States. Another instance when the default configuration might be changed is when the connection is a trunk to a PBX or key system. In that case, the FXS port must be configured to match the settings of that device.

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 the following configuration parameters:

- **signal:** Sets the signaling type for the FXS port. In most cases, the default signaling of loopstart 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 the system setting.

- **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 to the originating party.

- **description:** Configures a description for the voice port. You must use the description setting to describe the voice port in **show command** output. It is always useful to provide some information about the usage of a port. The description could specify the type of equipment that is connected to the FXS port.

- **ring frequency:** Configures a specific ring frequency (in Hz) 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 might buzz. In addition, the ring frequency is usually country-dependent, and you should take into account the appropriate ring frequency for your area before 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** setting 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.

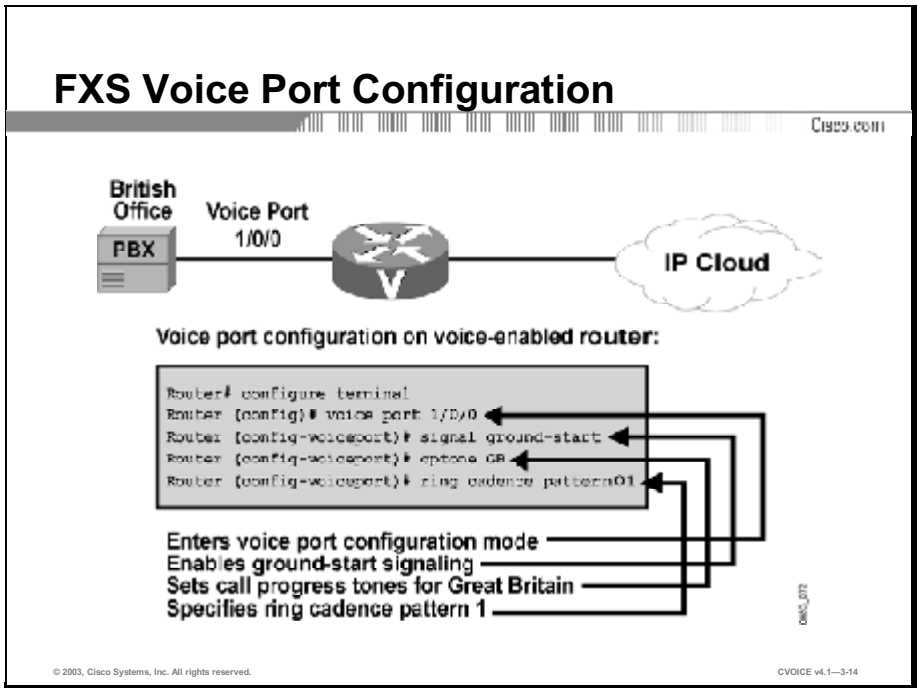
- **busyout:** Configures the ability to busy out an analog port.

- **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 and, if provided, will be used as the calling number if the call is originated from this voice port. If 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.

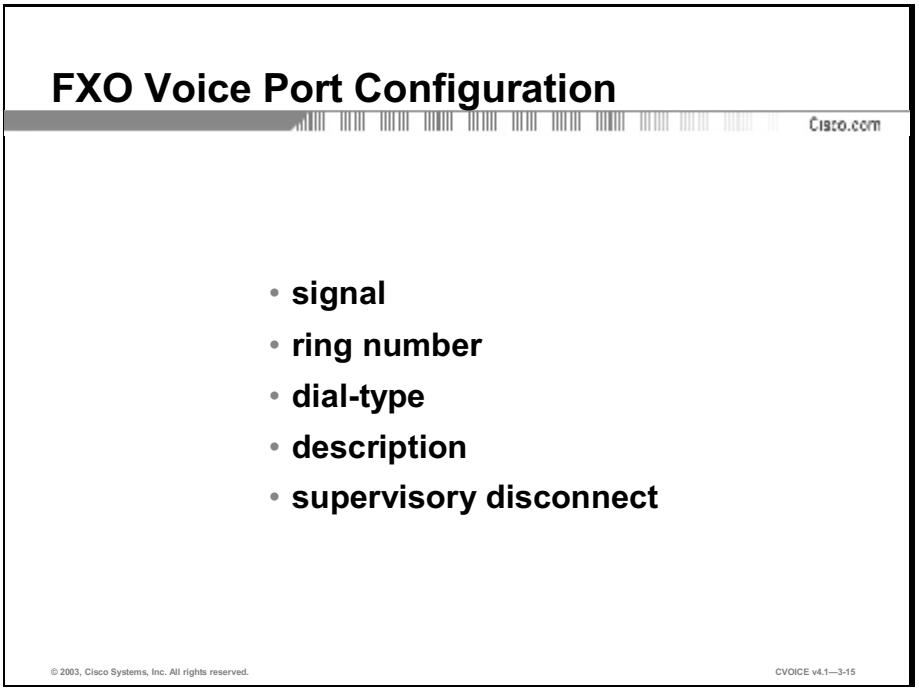
Example

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



Foreign Exchange Office 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.



Configuration Parameters

In most instances, the FXO port connection functions with default settings. FXO port configuration allows you to set parameters based on the requirements of the connection where default settings need to be altered or parameters set for fine-tuning. You can set the following 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.

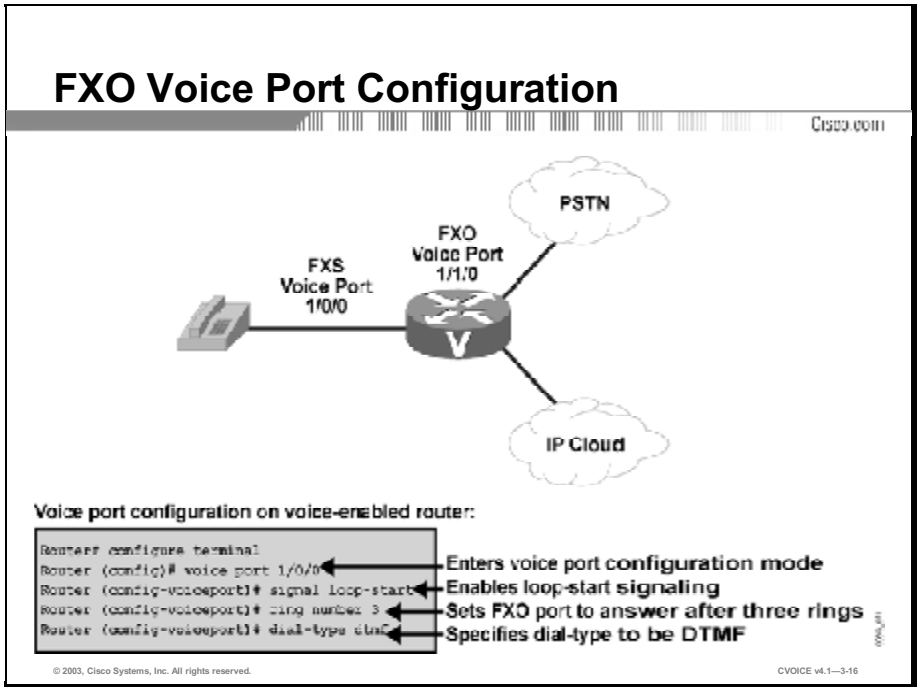
- **dial-type:** Configures the appropriate dial type for outbound dialing. Older PBXs or key sets may not support dual-tone multifrequency (DTMF) dialing. If you are connecting an FXO port to this type of device, you may need to set the dial type for pulse-dialing.

- **description:** Configures a description for the voice port. Use the description setting to describe the voice port in **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 verify the documentation to ensure that supervisory disconnect is supported.

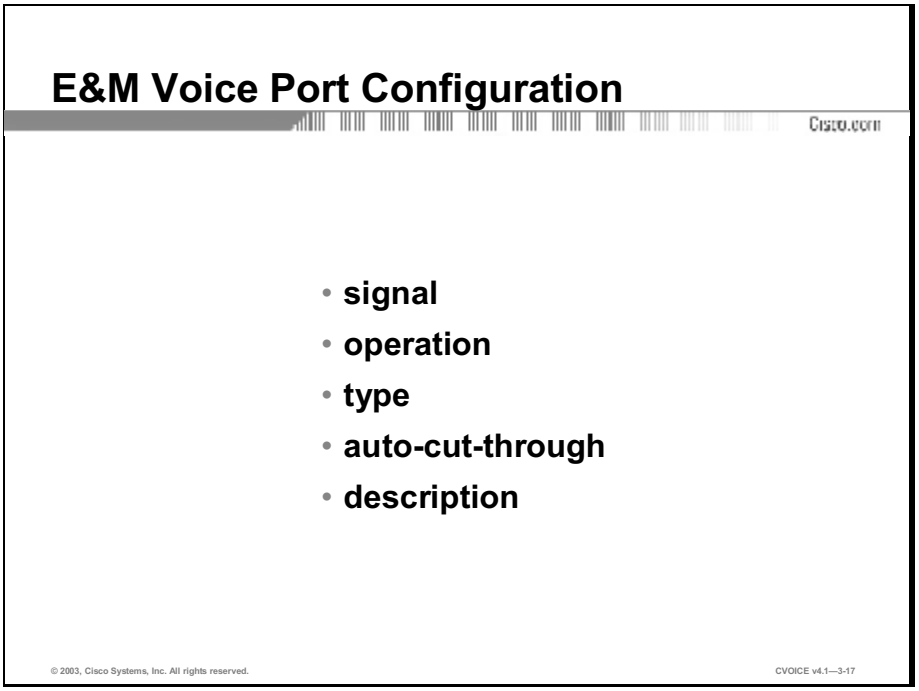
Example

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



Ear and Mouth Ports

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



Configuration Parameters

Although E&M ports have default parameters, you must usually configure these parameters to match the device that is connected to the E&M port. You can set the following 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 setting 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.

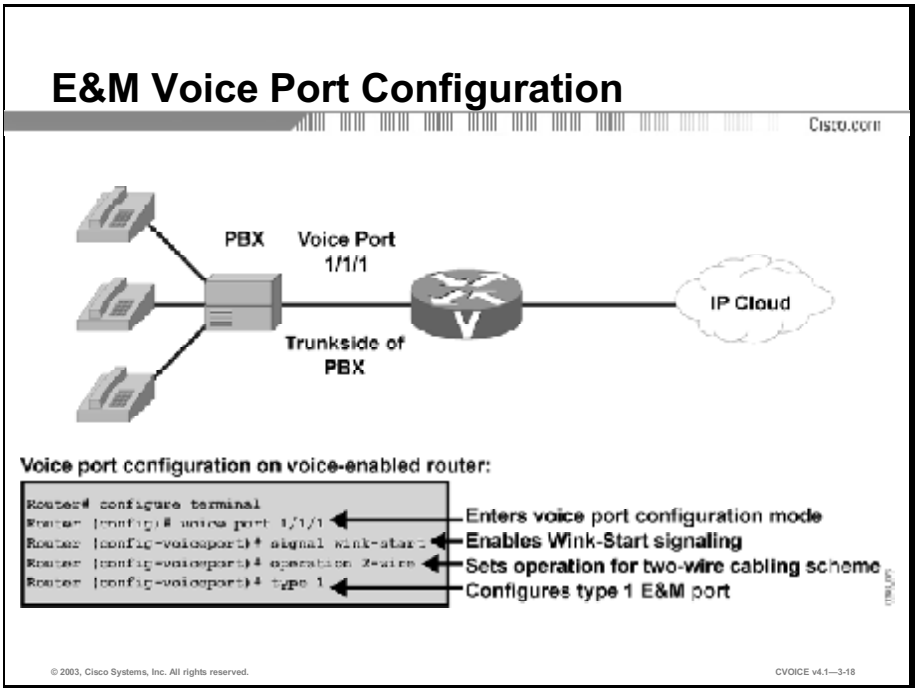
- **type:** Configures the E&M interface type for a specific voice port. The type defines the electrical characteristics for the E and M leads. The E and M leads are monitored for on-hook and off-hook conditions. From a PBX perspective, when the PBX attempts to place a call, it goes high (off hook) on 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.

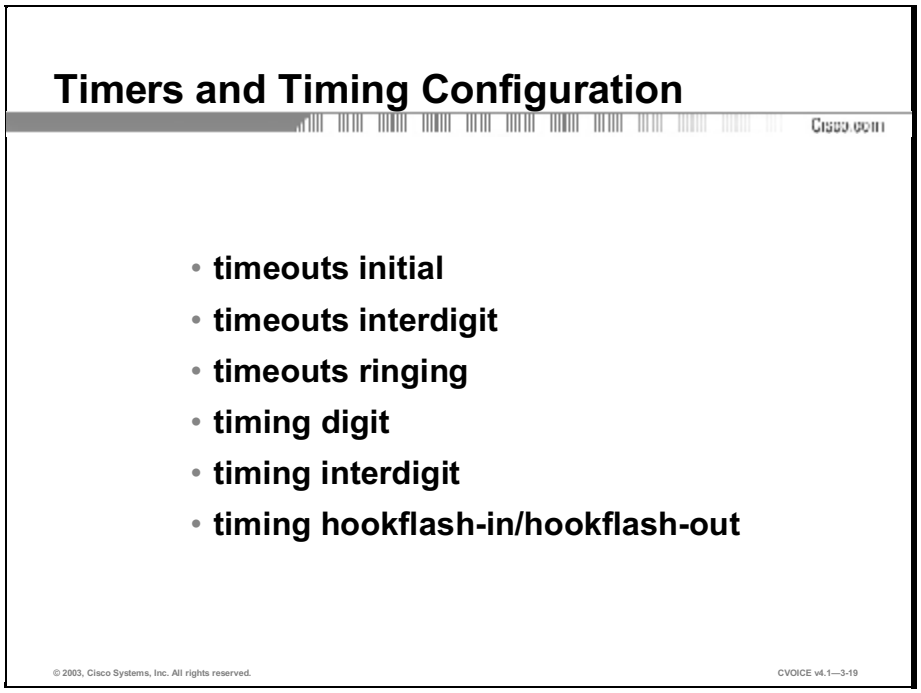
Example

The configuration in the figure enables Wink Start signaling on a Cisco 2600 or 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 adjusting. In instances where ports are connected to a device that does not properly respond to dialed digits or hookflash, or where the connected device provides automated dialing, these timers can be configured to allow more or less time for a specific function.



Configuration Parameters

You can set a number of timers and timing parameters for fine-tuning the voice port. Following 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 typically does not need to be changed.

- **timeouts interdigit:** Configures the number of seconds for which the system will wait (after the caller has input the initial digit) for the caller to input a subsequent digit of the dialed digits. 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 can continue ringing a telephone 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.

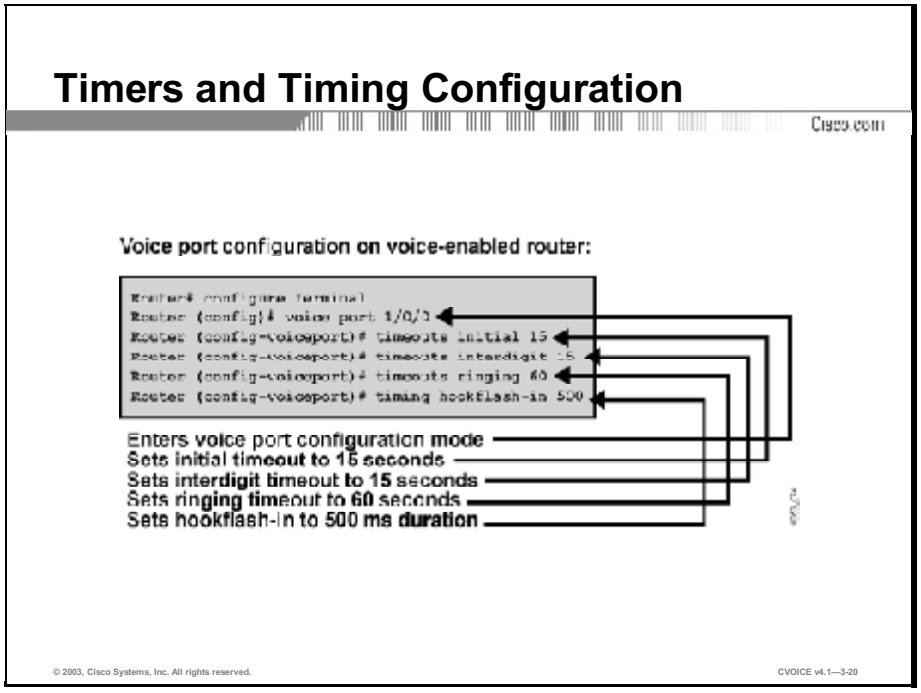
- **timing digit:** Configures the DTMF digit-signal duration for a specified voice port. You can use this setting to fine-tune a connection to a device that may have trouble recognizing dialed digits. If a user or device dials too quickly, the digit may not be recognized. By changing the timing on the 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 hookflash-in, 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 hookflash-out, 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.

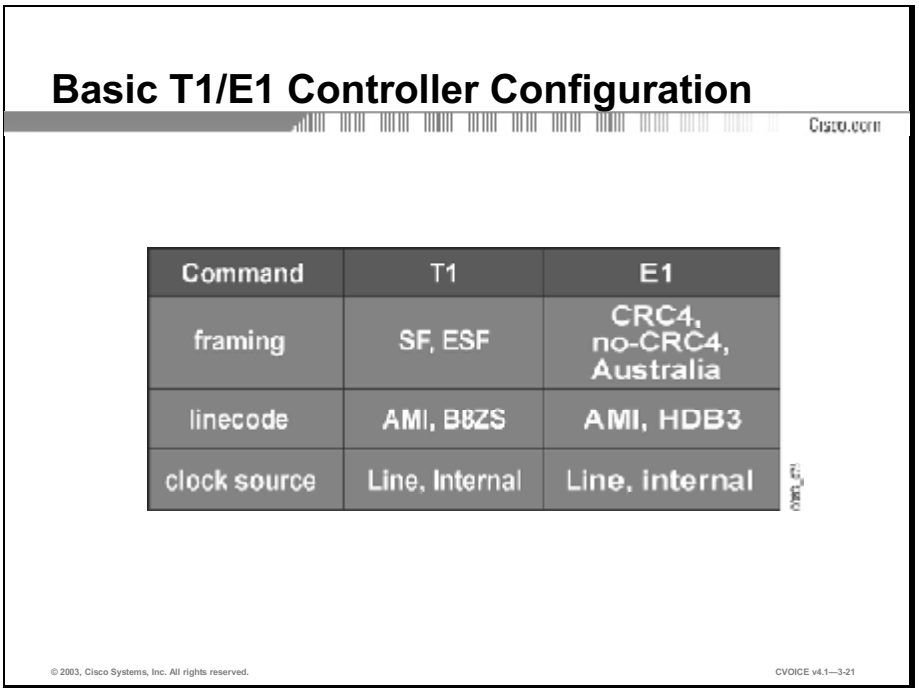
Example

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 only one minute. 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 13 minutes, and the hookflash-in timer is set to 500 ms.



Digital Voice Ports

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

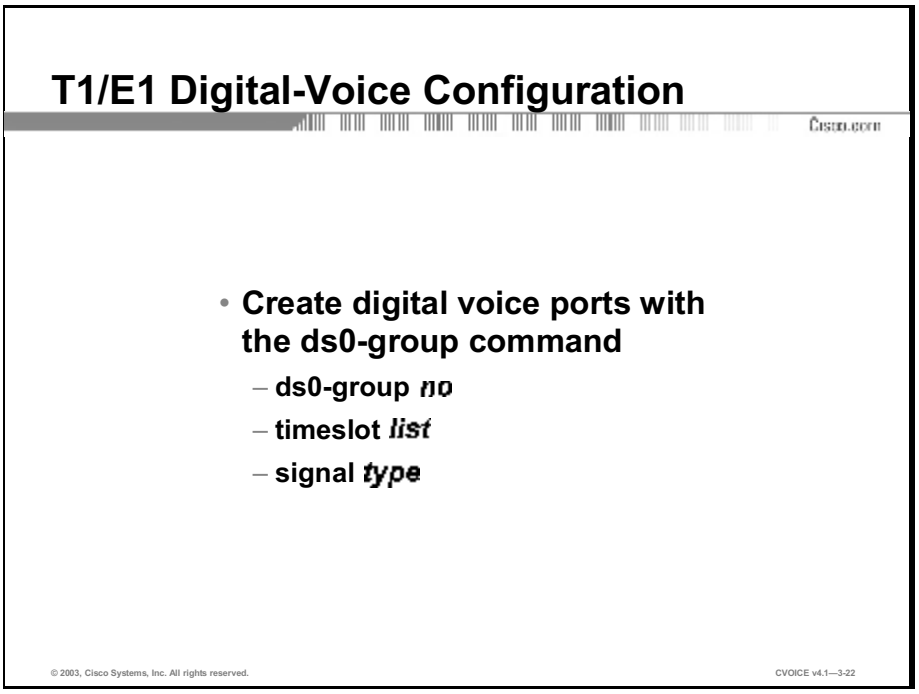


Configuration Parameters

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 following basic configuration parameters 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:** Superframe (SF) or Extended Superframe (ESF)
  - **Options for E1:** cyclic redundancy check (CRC4), no-CRC4, or Australia
  - **Default for T1:** SF
  - **Default for E1:** CRC4

- **linecode:** Configures the line-encoding format for the 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



You must create a digital voice port in the T1 or E1 controller to make the digital voice port available for specific voice port configuration 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* parameter identifies the 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* parameter is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas.

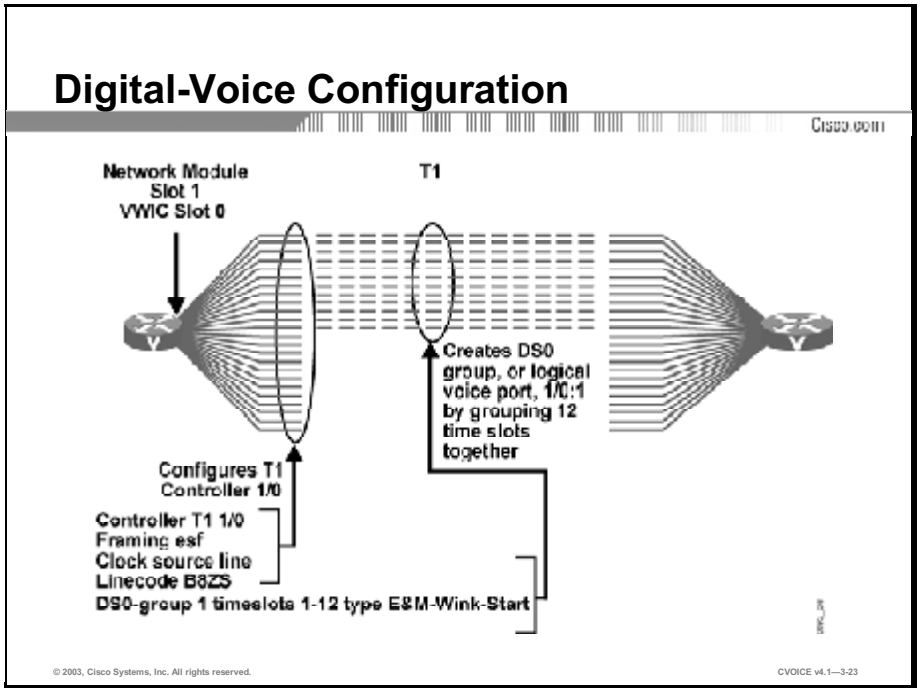
The **type** command defines the emulated analog signaling method that the router uses to connect to the PBX or PSTN. The type depends on whether the interface is T1 or E1.

After 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 a 2600 or 3600 platform, 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.

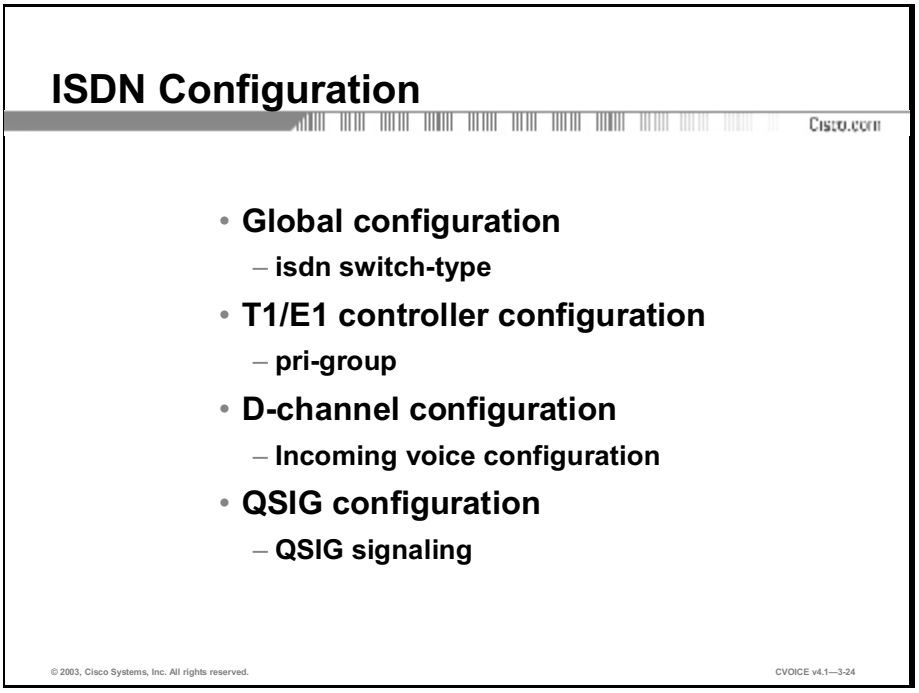
Example

This example configures the T1 controller for ESF, B8ZS linecode, 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* value 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.



Configuration Parameters

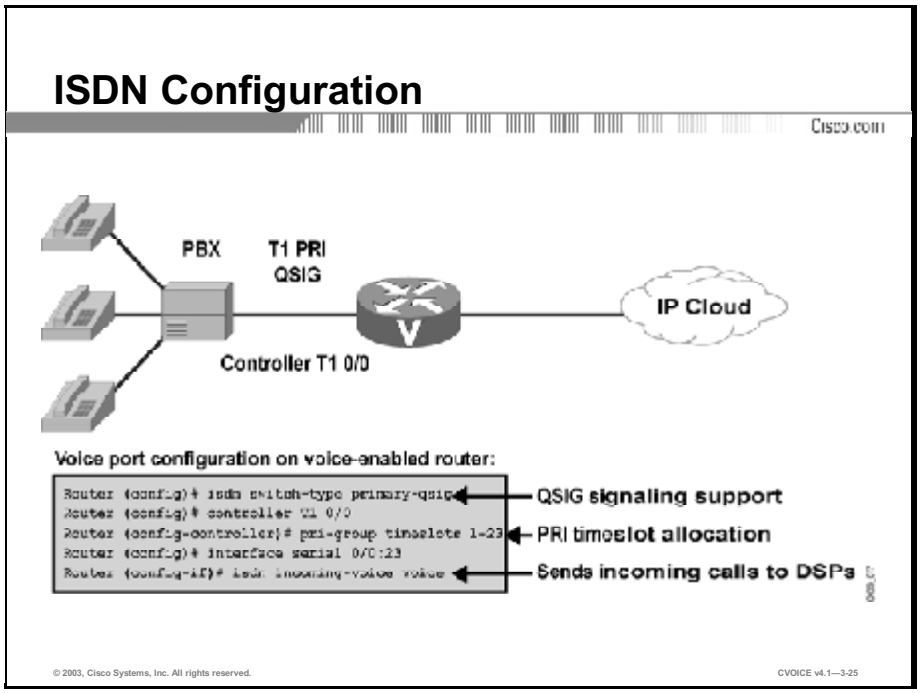
Cisco voice-capable devices provide support for both PRI and BRI voice connections. Many PBX vendors support either T1/E1 PRI or BRI connections. In Europe, where ISDN is more popular, many PBX vendors support BRI connections. When designing how the PBX passes voice to the network, you must ensure the router supports the correct connection. The first step in configuring ISDN capabilities for T1 or E1 PRI is to configure the T1 or E1 controller basics. After the clock source, framing, and linecode are configured, ISDN voice functionality requires the following 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 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 a select group of timeslots for the PRI group.
- **isdn incoming-voice 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.

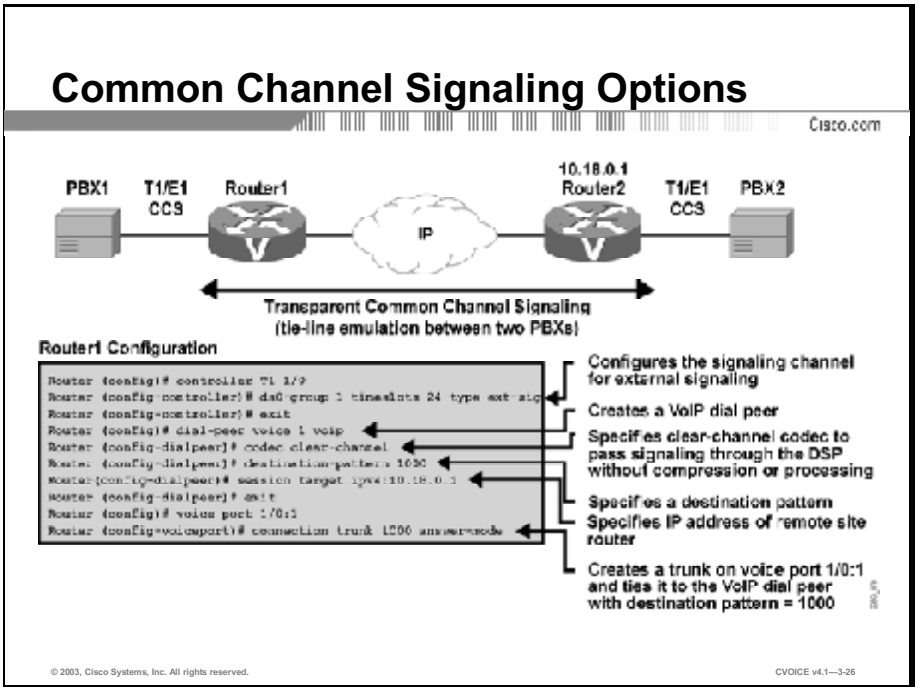
Example

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.



Common Channel Signaling 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 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 the following 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 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 PBX1 sends proprietary signaling across the signaling channel to Router1.

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

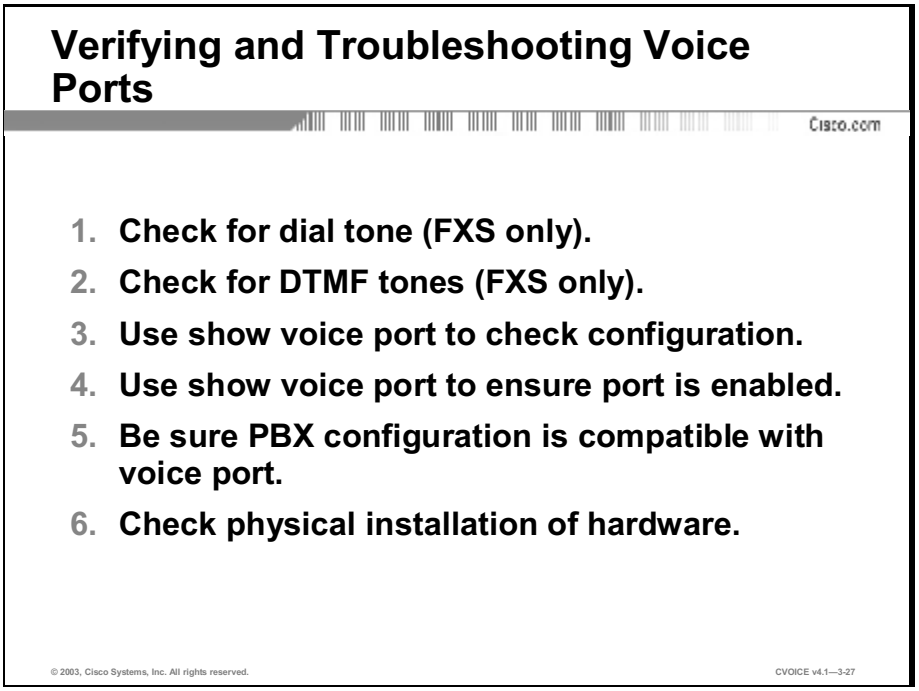
Step 3 The VoIP dial peer is configured for clear-channel codec and points to the IP address of the remote router (router 2) connecting the remote PBX (PBX2).

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 PBX2. The signal arrives at PBX2 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** and **test** commands that are used to monitor and troubleshoot voice ports.



You can perform the following 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?
Is the router running the correct version of Cisco IOS in order 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.

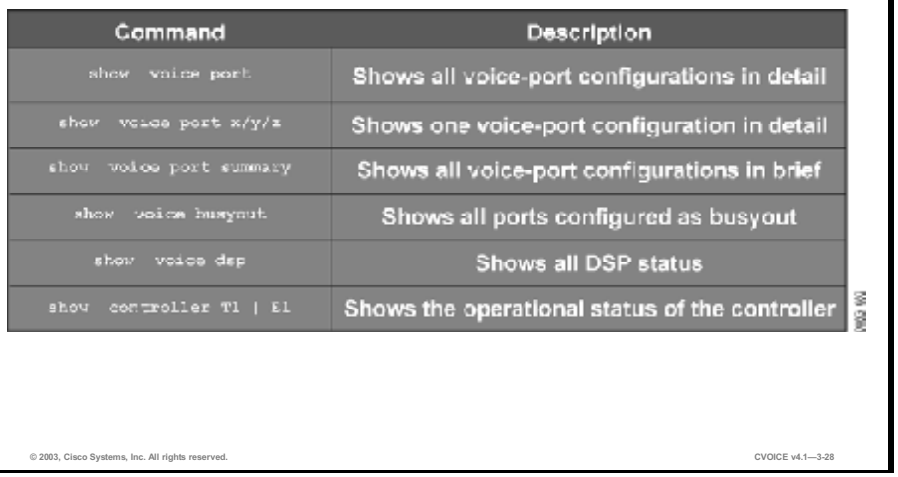
Step 3 Use the **show voice port** command to verify that the data configured is correct. If you have trouble connecting a call, and you suspect that the problem is associated with voice port configuration, you can try to resolve the problem by performing Steps 4 through 6.

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.

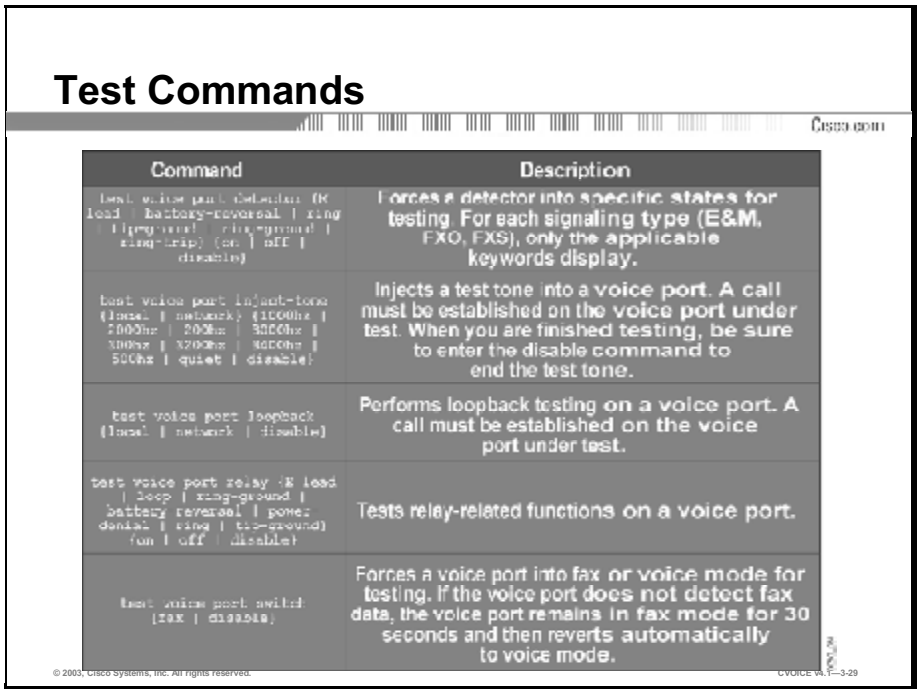
Step 5 If you have configured E&M interfaces, make sure that the values associated with your specific PBX setup are correct. Specifically, check for two-wire or four-wire Wink-Start, immediate-start, or delay-dial signal types, and the E&M interface type. These parameters need to match those set on the 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 card or with the module slot.

Commands to Verify Voice Ports



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

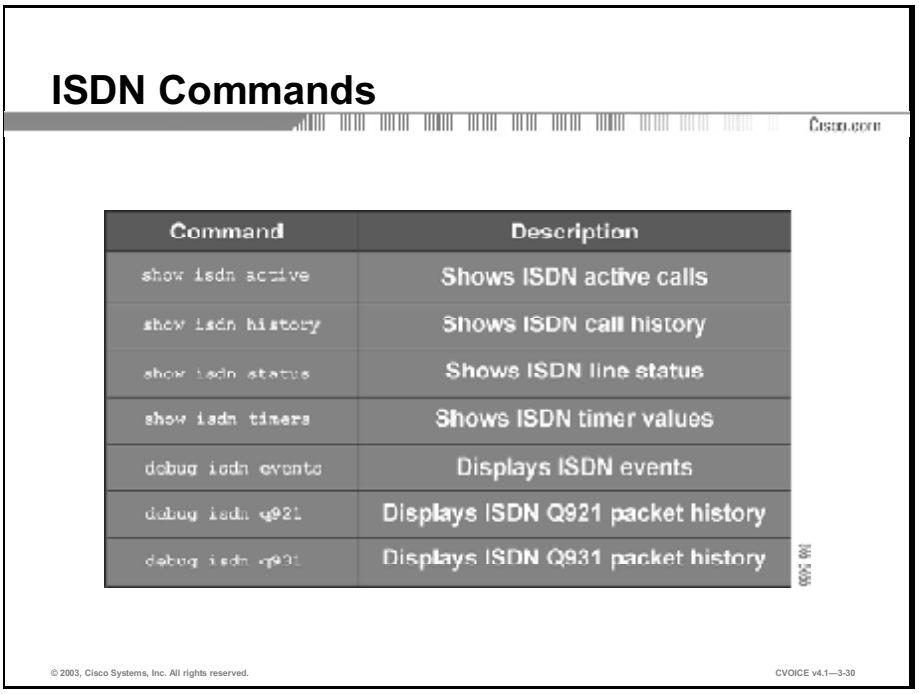


The **test** commands provide the ability to analyze and troubleshoot voice ports on the Cisco 2600 and 3600 routers. There are five **test** commands to force voice ports into specific states to test the voice port configuration.

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.

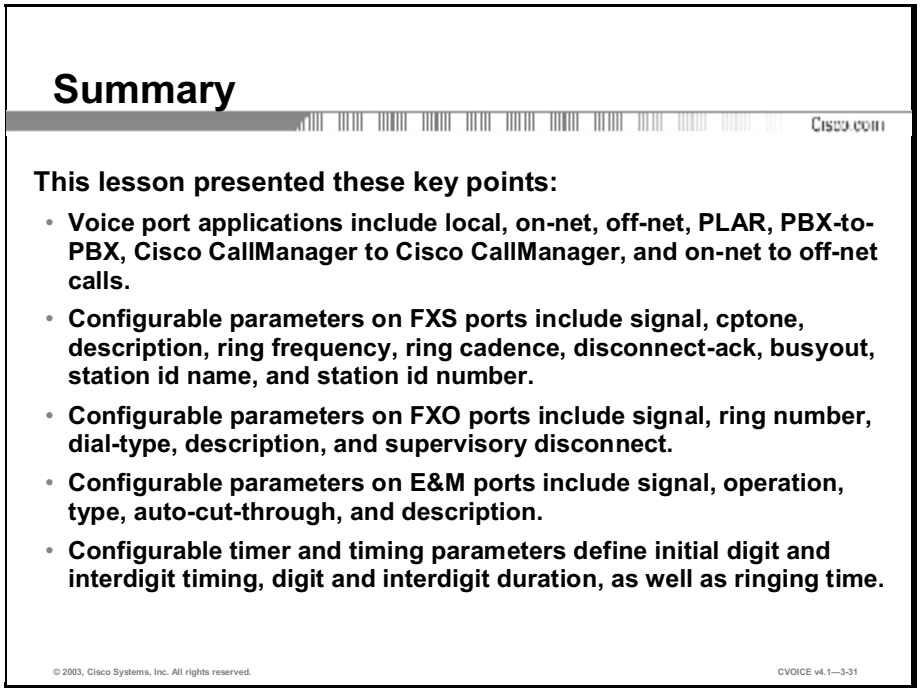
Note Refer to the *Voice Port Testing Enhancements in Cisco 2600 and 3600 Series Routers* document for further information.

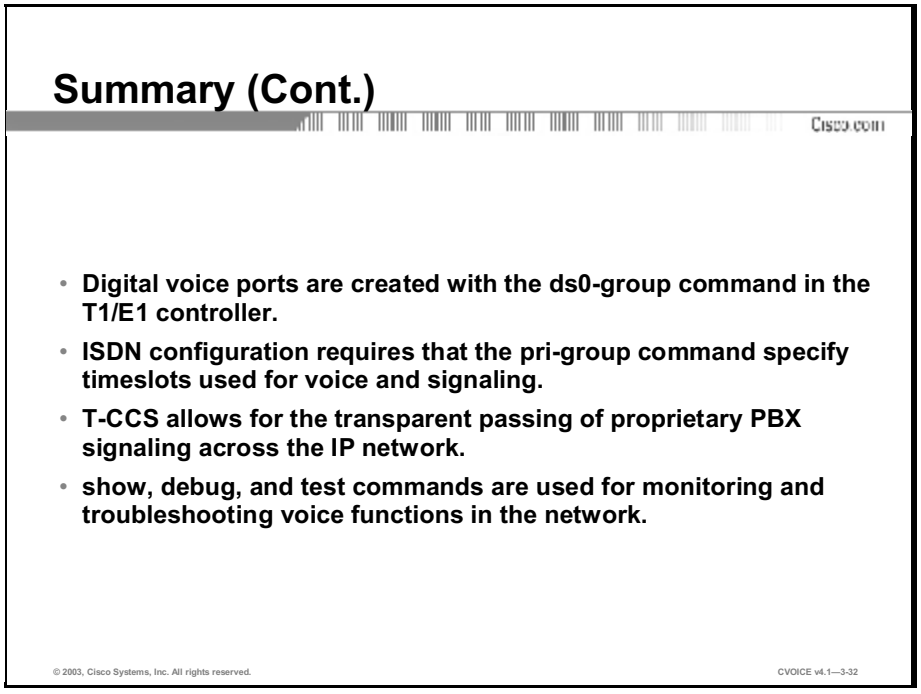


The ISDN **show** and **debug** commands in the figure are useful for viewing and troubleshooting ISDN connections.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Voice Port Configuration
- Assessment (Complex Lab): Refer to Lab 3-1, contained in Laboratory Exercises in Additional Resources section E.
- Adjusting Voice Quality lesson

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/fvvfax_c/vvfport.htm

Quiz: Voice Port Configuration

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Provide examples of seven types of voice port applications
- Set the configuration parameters for Foreign Exchange Station voice ports
- Set the configuration parameters for Foreign Exchange Office voice ports
- Set the configuration parameters for recEive and transMit 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 Transparent Common Channel Signaling in a Voice over IP environment
- Use the **show**, **debug**, and **test** commands to monitor and troubleshoot voice ports

Instructions

Answer these questions:

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 if you wanted to set the dial tone, the busy tone, and the ringback tone?

A) cptone

B) ring frequency

C) ring cadence

D) description

E) signal

Q4) Which situations would probably require you to change the FXS port default settings?

A) when the caller and the called party are in different parts of the country

B) when the caller and the called party are in different countries

C) when the connection is a trunk to a PBX

D) when the configuration of the FXS port matches the configuration of the local PSTN switch

Q5) Which statement 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 that is overseen by the network administrator

Q6) Which configuration parameter would you need to set for a device that does not support DTMF dialing?

A) **signal**

B) **dial type**

C) **description**

D) **supervisory disconnect**

Q7) What might happen if the wrong cable scheme is specified during E&M port configuration?

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) In which type of signaling does the router provide current on the E lead immediately upon seeing current on the M lead?

A) Delay-Start signaling

B) Immediate-Start signaling

C) Wink-Start signaling

D) Q signaling

Q9) Which parameter do you need to configure if you want to set the number of seconds the system should wait for the subsequent digit to be dialed after the caller has input the initial digit?

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 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) The configuration commands required for ISDN voice functionality include **isdn switch-type**, **isdn incoming-voice voice**, **qsig signaling**, and _____.

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) When you are configuring T-CSS in a VoIP network, the **trunk** [illegible] must match the number entered in the _____ 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) none of the above

Q18) Which two conditions can you check 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.

E) The signaling type matches the signaling type configured on the PBX.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Adjusting Voice Quality

Overview

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

Importance

User acceptance of the converged voice and data network depends on the quality of current calls compared to the quality through their original providers. As new devices are introduced in 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:

- Describe the electrical characteristics of analog voice and the factors affecting voice quality
- 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 fully benefit 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

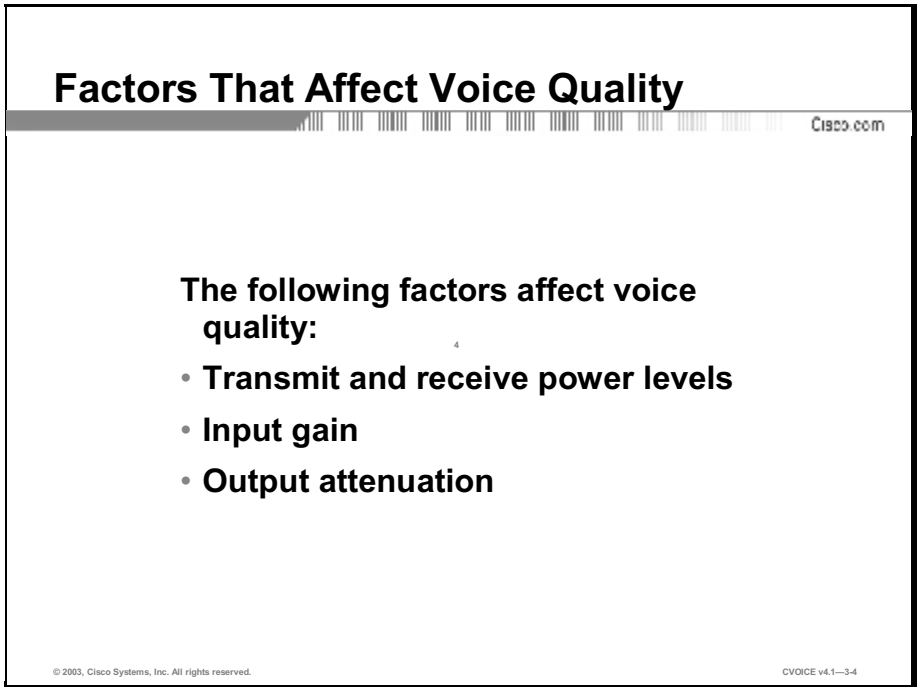
Outline

This lesson includes these topics:

- Overview
- Electrical Characteristics
- Voice Quality Tuning
- Echo Cancellation Commands
- Summary
- Assessment (Quiz): Adjusting Voice Quality
- Assessment (Complex Lab): Lab Exercise 3-1

Electrical Characteristics

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



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, and 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.

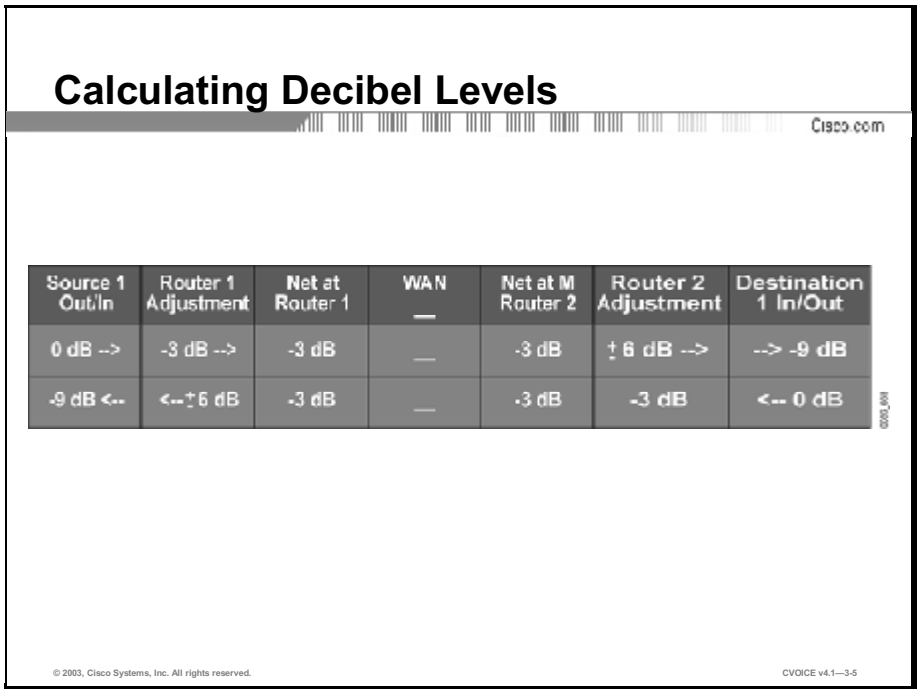
Another problem is inconsistent volume at different points in the network. Both echo and volume inconsistency may be caused by a voice port that is generating a signal level that is too high or too low. You can adjust signal strength, either in the inbound direction from an edge telephone or switch into the voice port, or 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. 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.

Calculating Decibel Levels

Change in signal strength is measured in decibels (dB). 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 dB level that device works best.

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



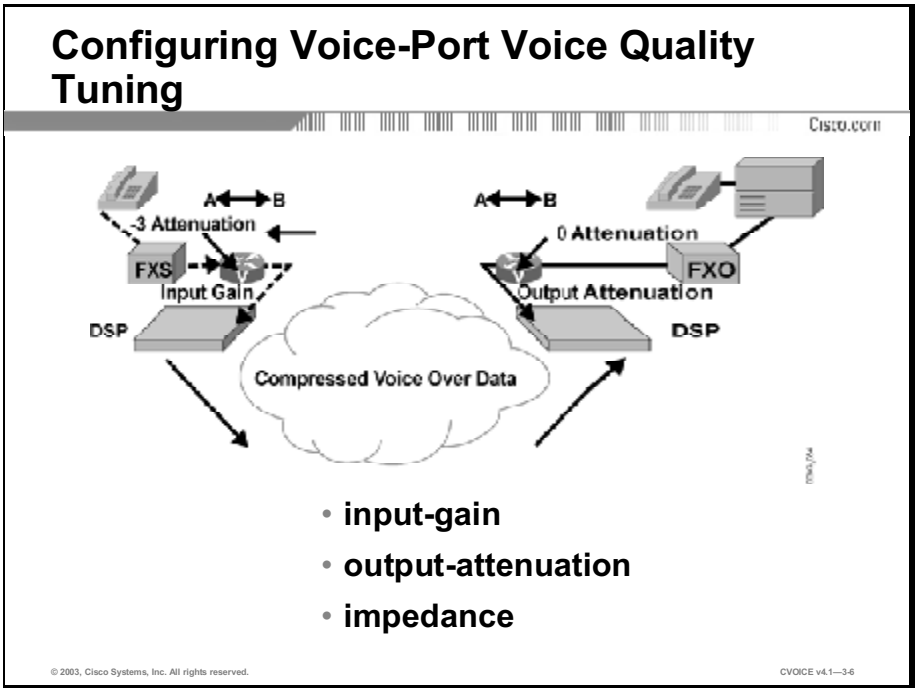
Baselining Input and Output Power Levels

Considerations for 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.

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 results 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 dB 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 -3dB. An analog telephone in North America and Europe works best with a receive level of -9dB.Therefore, if the device connecting to that router provides a different level than the expected -3dB, then input gain can be set to equalize it to -3dB. If the output at the other end is a telephone that expects -9 dB, then 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 -9dB levels. A system-wide loss plan looks at the dB 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 dB levels and assumes that interfaces already provide the expected dB 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.

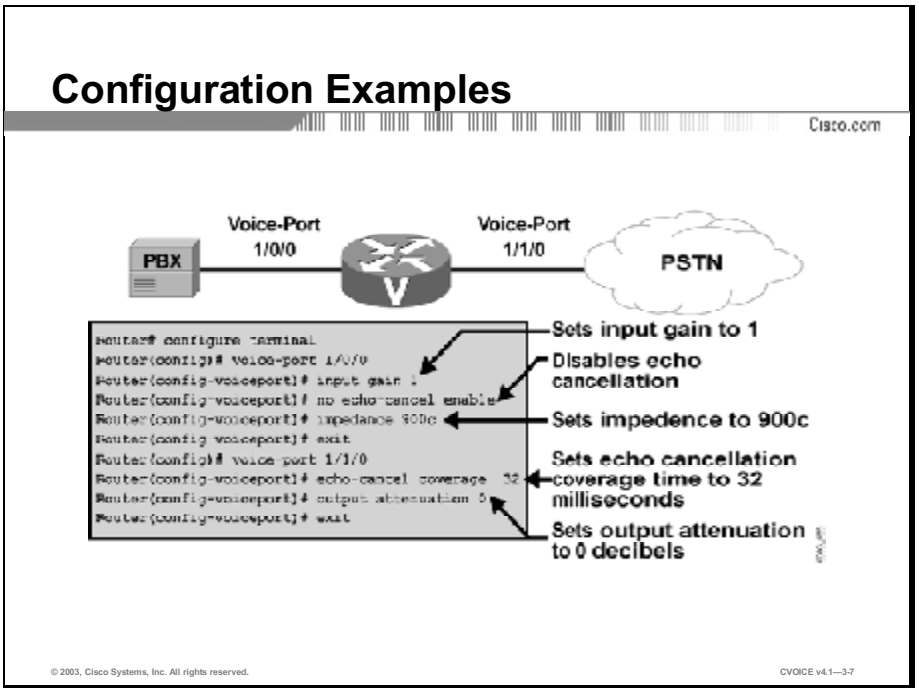
- **output-attenuation:** Configures the output attenuation value in decibels for the transmit side. The value represents the amount of loss to be inserted at the transmit side of the interface.

- **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 600r. PBXs in the United States are normally 600r or 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. In addition, 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



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 600r to match the 900c 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.

E&M voice port parameters include:

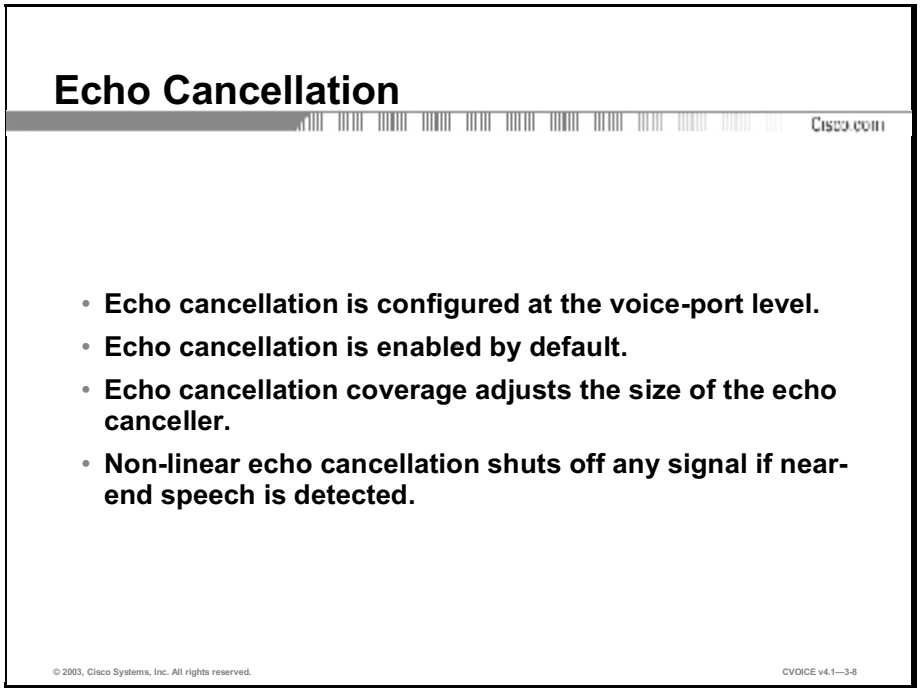
- **input-gain:** Increases the inbound voice level by 1 dB before the voice is transmitted across the network
- **no echo-cancel enable:** Disables echo cancellation
- **impedance:** Sets the impedance to match the connecting hardware

FXO voice port parameters include:

- **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 is configured at the voice port level. It is on by default and its characteristics are configurable. Considerations for echo cancellation commands are as follows:

- **echo-cancel enable:** Enables cancellation of voice that is sent out through the interface and received back on the same interface. Sound that is received back in this manner 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 recEive and transMit or ear and mouth (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:** 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 connected 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; for example, the non-plain old telephone service (POTS) side of the connection.

Note	This command is valid only if the echo cancel feature has been enabled.

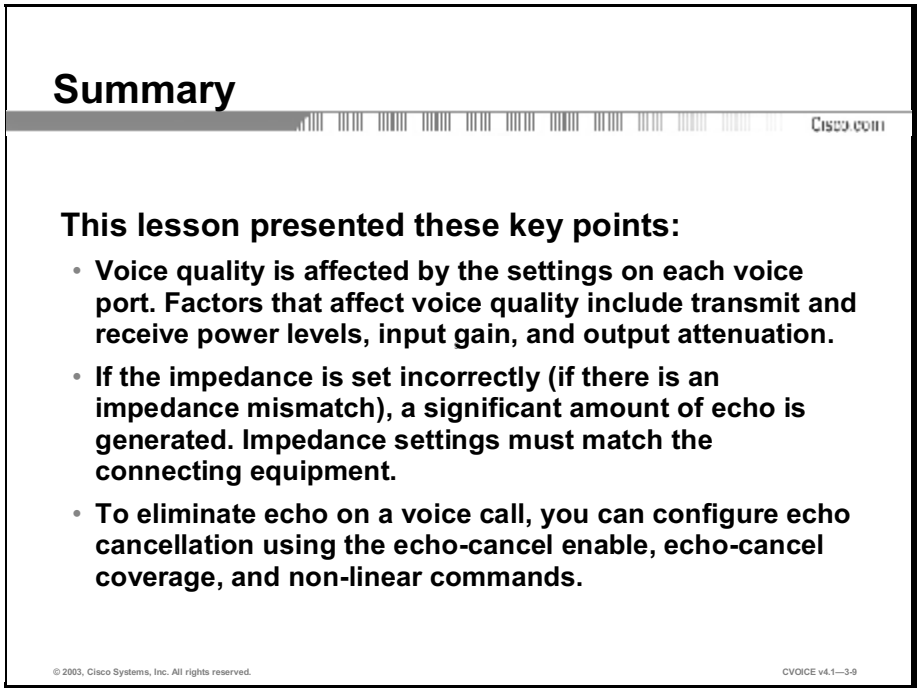
- **non-linear:** The function enabled by the **non-linear** command is also known as residual echo suppression. This command effectively creates a half-duplex voice path. If voice is present on the inbound path, then there is no signal on the outbound path. This command is associated with the echo canceller operation. The **echo-cancel enable** command must be enabled for the **non-linear** command to take effect. 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 non-linear 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.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Adjusting Voice Quality
- Assessment (Complex Lab): Refer to Lab 2-1, contained in Laboratory Exercises in Additional Resources section E.
- Voice Dial Peers module

References

For additional information, refer to these resources:

- "Voice Quality Tuning Commands" http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfport.htm#56672

Quiz: Adjusting Voice Quality

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the electrical characteristics of analog voice and the factors affecting voice quality
- Configure voice port parameters to fine-tune voice quality
- Configure echo cancellation on the voice ports to improve voice quality

Instructions

Answer these questions:

Q1) Which factor can cause echo during transmission of voice over an IP network?

A) incorrect input levels

B) incorrect output levels

C) impedance mismatch

D) all of the above

Q2) Analog voice routers operate best when the receive level from an analog source is set at _____.

A) -2 dB

B) -3 dB

C) -9 dB

D) -14 dB

Q3) Which two parameters 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

Q4) What 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

Q5) Which command is used to suppress listener echo?

A) echo-cancel enable

B) echo-cancel coverage

C) non-linear

D) no echo-cancel enable

Q6) Which of these commands is enabled by default?

A) echo-cancel enable

B) echo-cancel coverage

C) non-linear

D) no echo-cancel enable

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

4

Voice Dial Peers

Overview

Configuring dial peers is the key to setting up dial plans and implementing voice over a packet network. A router may need to manipulate digits in a dial string before it passes the dial string to a telephony device. This module discusses dial-peer configuration, hunt groups, digit manipulation, and special-purpose connections.

Upon completing this module, 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, given the definition of call legs
- Describe the proper use of digit manipulation and configuration of dial peers to implement a successful Voice over IP network, when provided the use and type of dial peers
- Configure voice ports for connection types necessary to integrate Voice over IP technologies with legacy PBXs and public switched telephone networks correctly, given the definition of special-purpose connection types

Outline

The module contains these lessons:

- Call Establishment Principles
- Dial Peers
- Special-Purpose Connections

Call Establishment Principles

Overview

This lesson describes call flows as they relate to inbound and outbound dial peers.

Importance

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.

Objectives

Upon completing this lesson, you will be able to:

- Describe call legs and their relationships to other components
- Describe how call legs are interpreted by routers to establish end-to-end calls

Learner Skills and Knowledge

To fully benefit 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

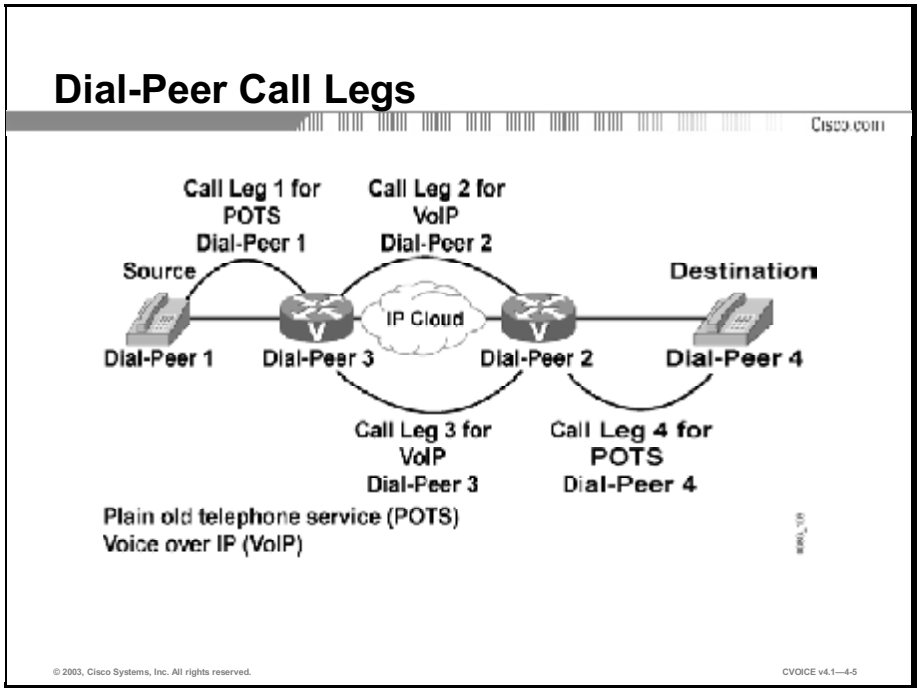
Outline

This lesson includes these topics:

- Overview
- What Are Call Legs?
- End-to-End Calls
- Summary
- Assessment (Quiz): Call Establishment Principles

What Are 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.

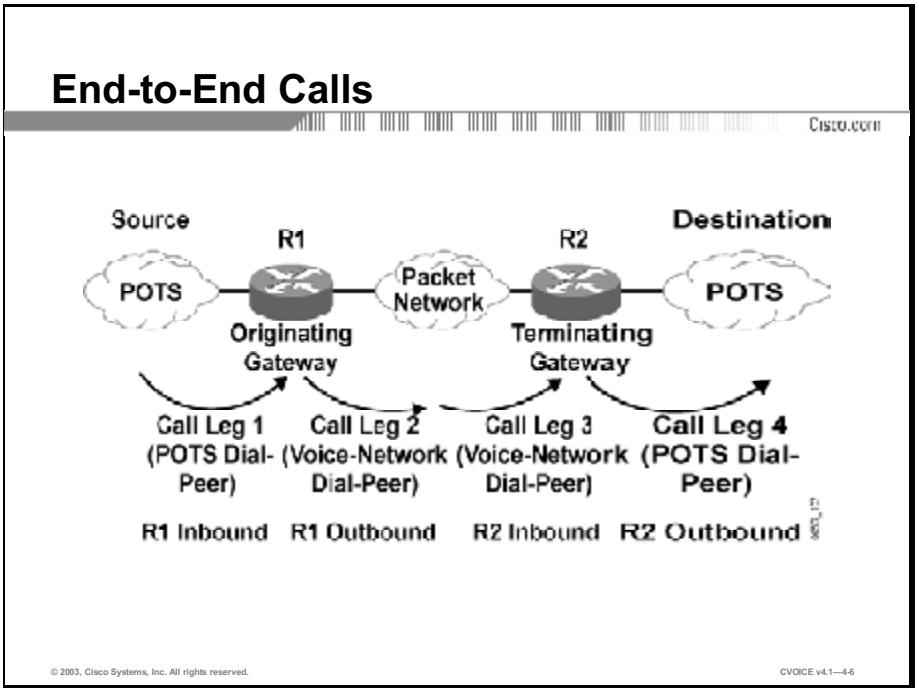
Example

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. When the call is established, dial peers are no longer used.

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) or gateway perspective. An inbound call leg originates when an incoming call comes *into* the router or gateway. An outbound call leg originates 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 below:

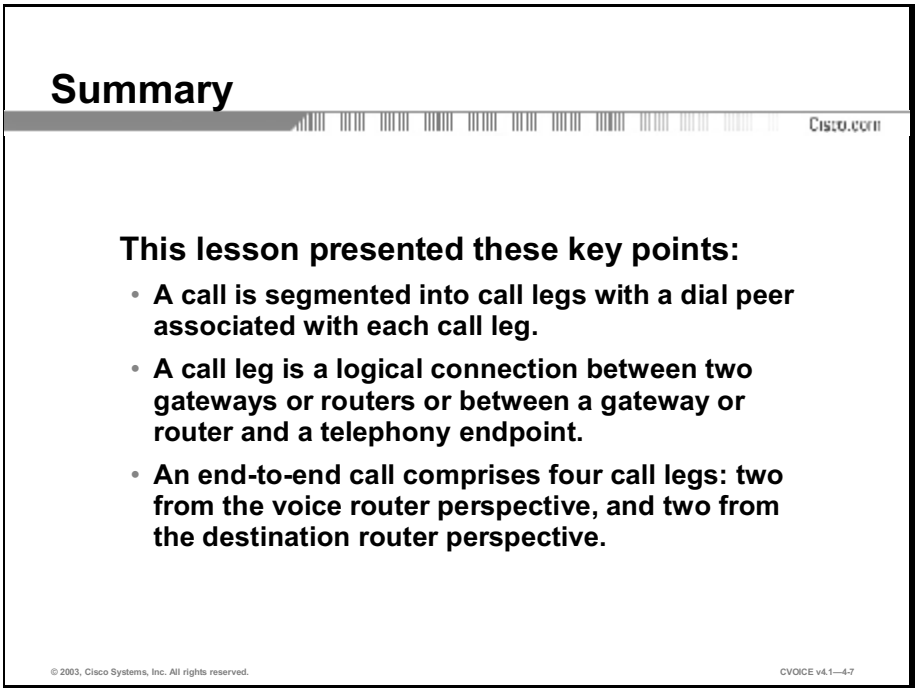
1. The plain old telephone service (POTS) call arrives at R1 and an inbound POTS dial peer is matched.
2. After associating the incoming call to an inbound POTS dial peer, R1 creates an inbound POTS call leg and assigns it a Call ID (Call Leg 1).
3. R1 uses the dialed string to match an outbound voice 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 Router 2 (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.

When the originating router or gateway requests non-default capabilities or applications, 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).

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Call Establishment Principles
- Dial Peers lesson

References

For additional information, refer to these resources:

- "Voice—Understanding Inbound and Outbound Dial Peers on Cisco IOS Platforms" http://www.cisco.com/warp/public/788/voip/in_out_dial_peers.html

Quiz: Call Establishment Principles

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe call legs and their relationships to other components
- Describe how call legs are interpreted by routers to establish end-to-end calls

Instructions

Answer these questions:

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 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 non-default voice capabilities?

A) It negotiates with the originating router until the default capabilities are accepted.

B) It reconfigures the ports to meet the requested capabilities.

C) It matches an inbound voice network dial peer that has the requested capabilities.

D) It terminates the call.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

Dial Peers

Overview

This lesson describes voice dial peers, hunt groups, digit manipulation, and the matching of calls to dial peers.

Importance

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 dial peers and their application
- Configure plain old telephone service 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
- List hunt group commands

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

Learner Skills and Knowledge

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

- Familiarity with Cisco IOS® commands
- Familiarity with telephony concepts

Outline

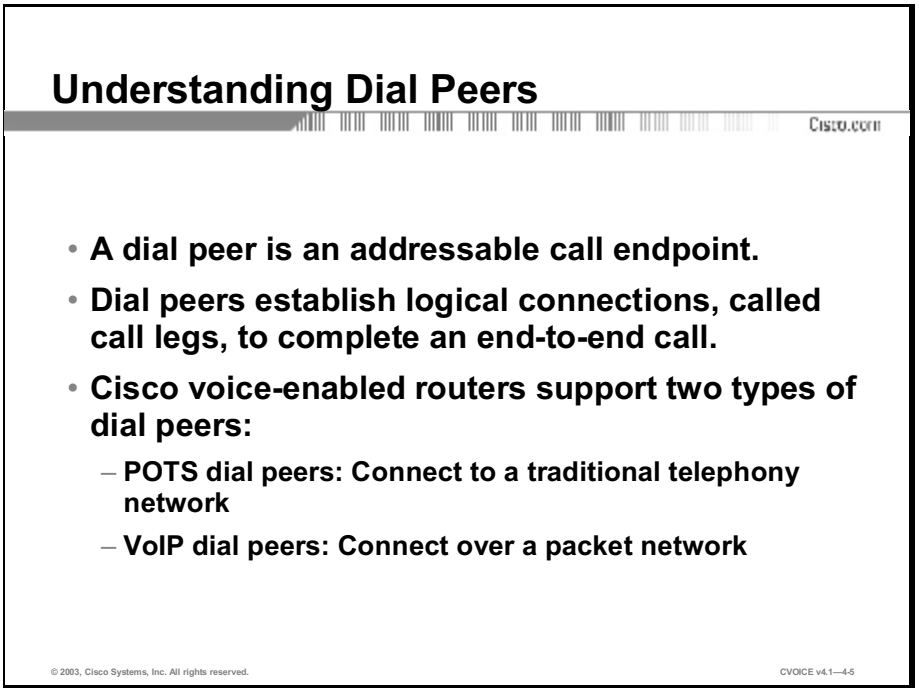
This lesson includes these topics:

- Overview
- What Is a Dial Peer?
- Configuring Plain Old Telephone Service Dial Peers
- Configuring VoIP Dial Peers
- Destination-Pattern Options
- What Is the Default Dial Peer?
- Matching Inbound Dial Peers
- Matching Outbound Dial Peers
- Hunt Group Commands
- Configuring Hunt Groups
- Digit Collection and Consumption
- What Is Digit Manipulation?

- Summary
- Assessment (Quiz): Dial Peers
- Assessment (Complex Lab): Lab Exercise 4-1

What Is a Dial Peer?

This topic describes dial peers and their applications.



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 have a way to decide whether the call can be routed, and where the call can be sent. The router does this by looking through 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 only 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.

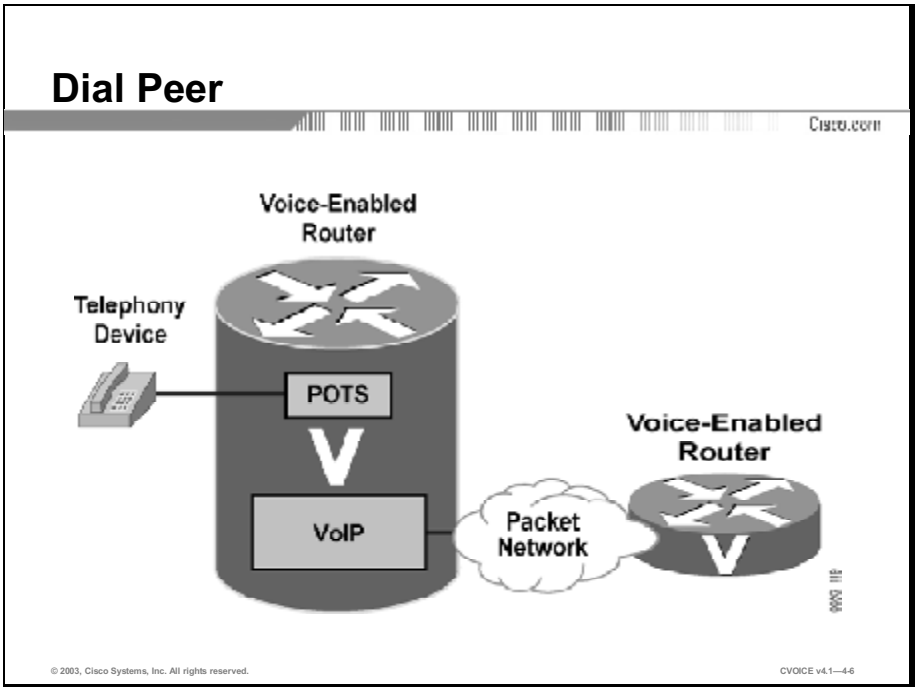
Dial peers define the parameters for the calls that they match. For example, if a call is originating and terminating at the same site, and is not crossing through slow speed WAN links, then the call can cross the local network uncompressed and without special priority. A call that originates locally and crosses the WAN link to a remote site may require compression with a specific 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 Systems voice-enabled routers support two types of dial peers:

- **Plain old telephone service (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
- **Voice over IP (VoIP) dial peers:** Connect over a packet 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

This figure shows a dial-peer configuration.



In the figure, the telephony device connects to the Cisco Systems voice-enabled router POTS dial. The POTS dial-peer configuration includes the telephone number of the telephony device and the voice port to which it is attached. The router knows 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.

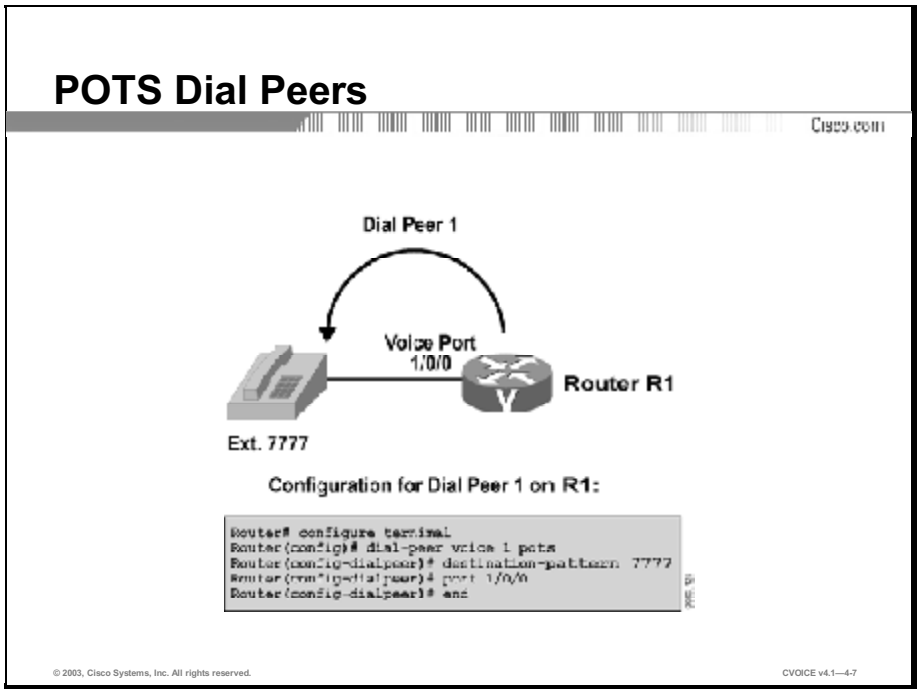
Follow the steps to place a VoIP call:

Table 1: How to Place a VoIP Call

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

Configuring Plain Old Telephone Service Dial Peers

This topic describes how to configure POTS dial peers.



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 to configure POTS dial peers:

Table 2: 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.

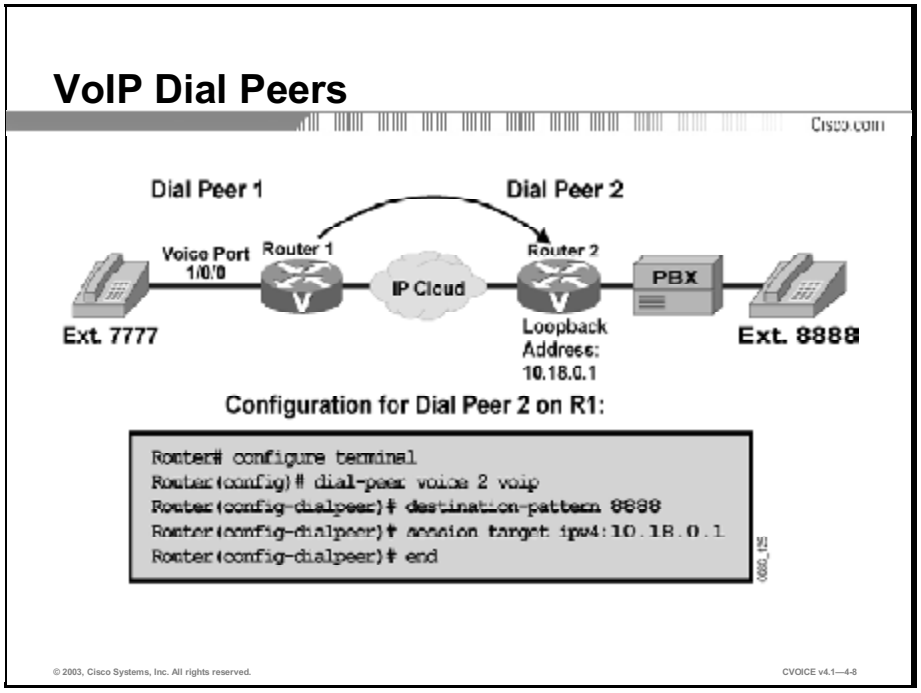
The dial peer type will be specified as POTS because the edge device is directly connected to a voice port and the signaling must be sent from this port to reach the device. There are two basic parameters that need to be specified for the device: the telephone number and the voice port. When a PBX is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

Example

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, voice port 0.

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, 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 these steps to configure VoIP dial peers:

Table 3: 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
4	Use the **destination-pattern** command to configure a range of numbers reachable by the remote router or gateway
5	Use the **session target** command to specify an IP address of the terminating router or gateway
6	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 parameters that are specified in the dial peer. The dial peer must then package it as an IP packet for transport across the network. Specified parameters may include the codec used compression (VAD, for example), or marking the packet for priority service.

The destination-pattern parameter 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 parameter 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 that can return an IP address of that remote terminating device.

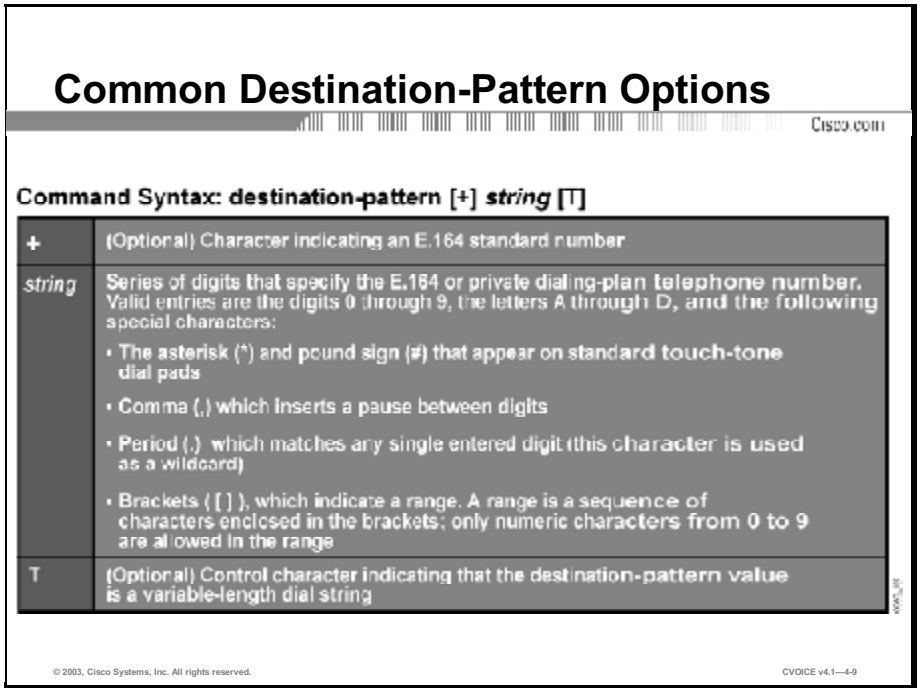
To determine which IP address a dial peer should point to, it is recommended that you use a loopback address. The loopback address is always up on a router, as long as the router is powered on and the interface is not administratively shut down. If an interface IP address is used instead of the loopback, and that interface goes down, the call will fail even if there is an alternate path to the router.

Example

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.

Destination-Pattern Options

This topic describes destination-pattern options and the applicable shortcuts.



The destination pattern associates a telephone number with a given dial peer. The destination pattern 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 or a partial telephone number with wildcard digits; it can also point to a range of numbers defined in a variety of ways.

Destination-pattern options include:

- **Plus (+):** An optional character that indicates an E.164 standard number. E.164 is the International Telecommunication Union Telecommunication Standardization Sector (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 Recommendation E.164.

- ***String:*** A series of digits specifying the E.164 or private dialing-plan telephone number. The examples below show the use of special characters that are often found in destination patterns strings:

  - 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.

  - Comma (,) inserts a one-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.

  - Period (.) matches any single entered digit (this character is used as a wildcard). The wildcard is used to specify a group of numbers that may be accessible via a single destination router, gateway, PBX or Cisco Call Manager. Because the period (commonly referred to as a dot), indicates a single digit of 0 to 9, this limits how efficiently ranges of numbers are used. A pattern of "200." allows for 10 uniquely addressed devices, where 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, then 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].". The bracket notation offers much more flexibility in how numbers can be assigned.

- **T:** 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, then 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 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.

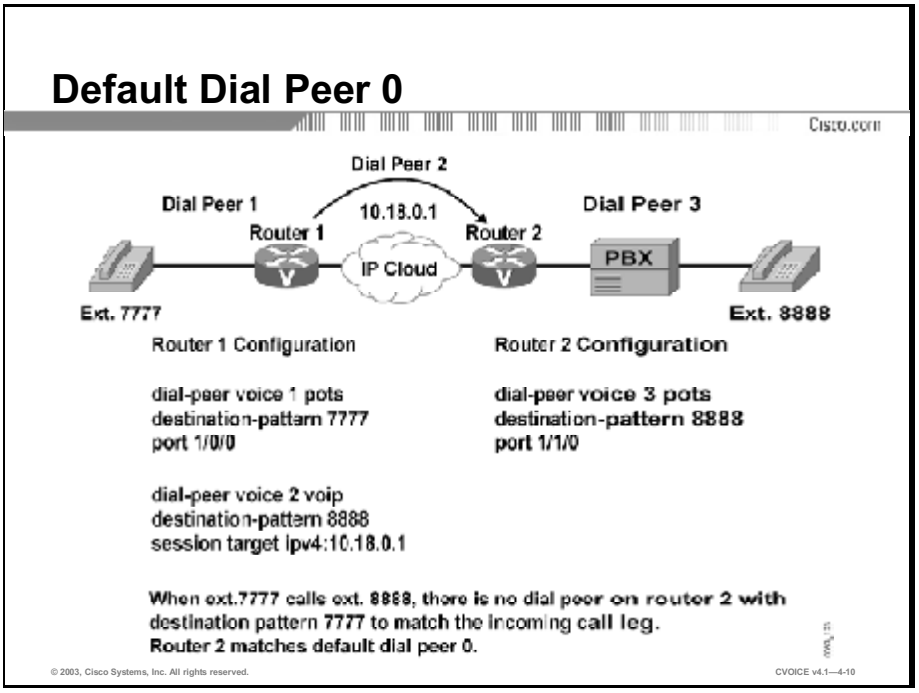
Example

Table 4: Example: Destination-Pattern Options

Destination Pattern	Matching Telephone Numbers
5551234	Matches one telephone number exactly, 5551234. This is typically used when there is a single device, such as a telephone or fax, connected to a voice port.
555[1-3]…	Matches a seven-digit telephone number where the first three digits are 555, the fourth digit can be a 1, 2, or 3, and the last digits can be any valid digits. This type of destination pattern is used where 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 thirty numbers assigned.
.T	Matches any telephone number that has at least one digit and can vary in length from 1 to 32 digits total. This destination pattern is used for a dial peer that services a variable-length dial plan, such as 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 one and can be directed to an operator.

What Is the 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

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 towards 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	There is an exception to the previous statement. Cisco voice and/or dial platforms, such as the AS53*xx* and AS5800, 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 dial-up (modem) call.

Dial-peer 0 for inbound VoIP peers has the following configuration:

- any codec
- ip precedence 0
- vad enabled
- no rsvp support
- fax-rate service

Dial-peer 0 for inbound POTS peers has the following configuration:

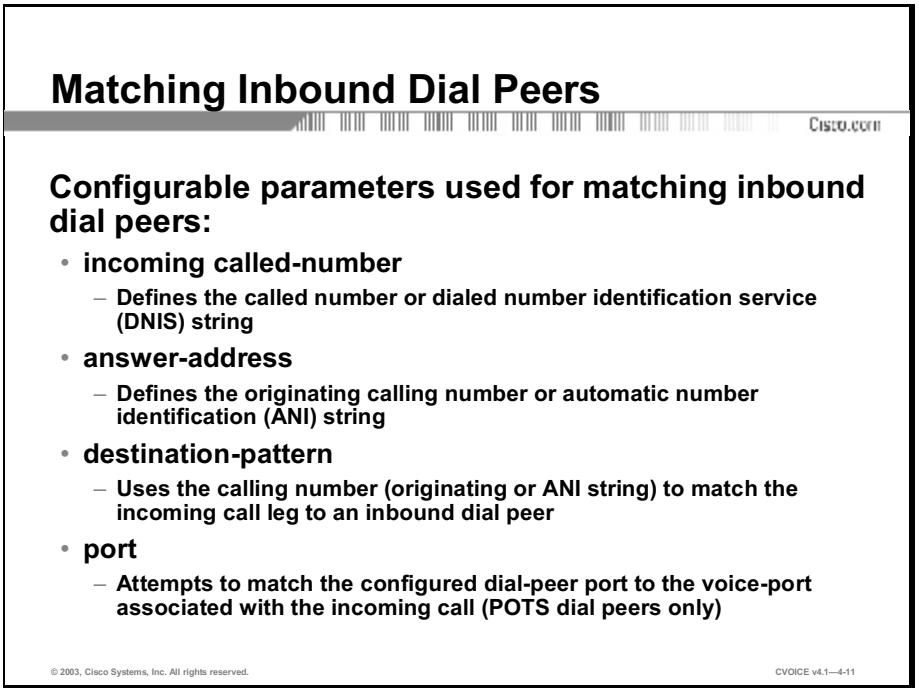
- no ivr application

You cannot change the default configuration for dial-peer 0. Default dial-peer 0 fails to negotiate non-default 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, 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. In this example, VAD is *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 inbound dial peers.



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 to the incoming POTS call legs of the originating router or gateway.
- Inbound VoIP dial peers are associated to 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 three call setup information elements are:

Table 5: 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 (CAS) 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 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 makes 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 following order:

Table 6: 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** 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 **answer-address** 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** 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, then the router or gateway matches the first dial peer added to the configuration
6	If a match is not found in the previous steps, then the default is dial-peer 0

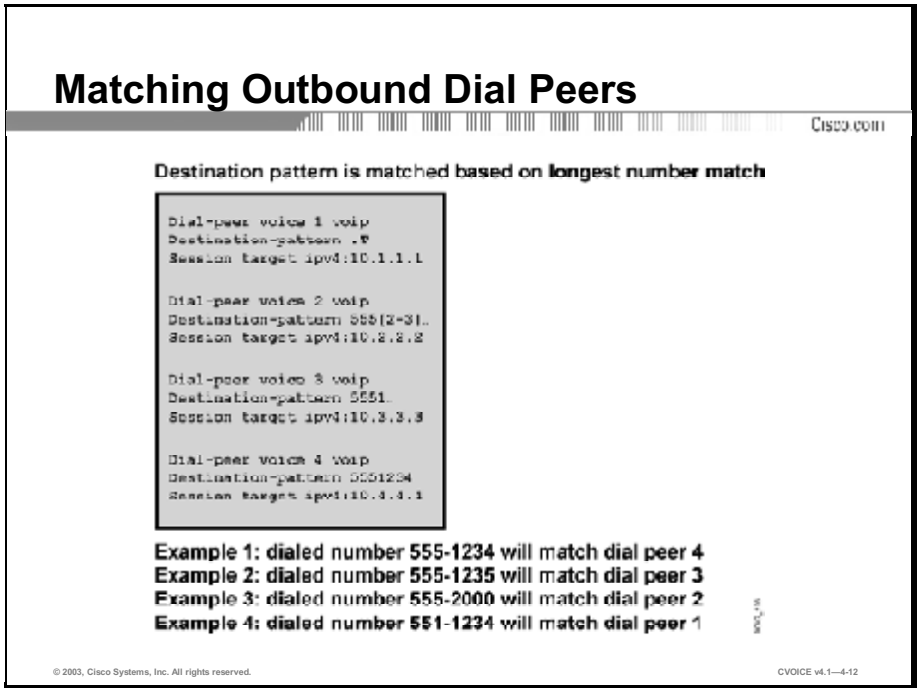
Because call setups always include DNIS information, it is recommended that you use the **incoming called-number** command for inbound dial-peer matching. Configuring **incoming called-number** is useful for a company that has a central call center providing support for a number of different products. Purchasers of each product get a unique 1-800 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** 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 **destination pattern** 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.

Matching Outbound Dial Peers

This topic describes how the router matches outbound dial peers.



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 following order:

Table 7: How the Router or Gateway Matches Outbound Dial Peers

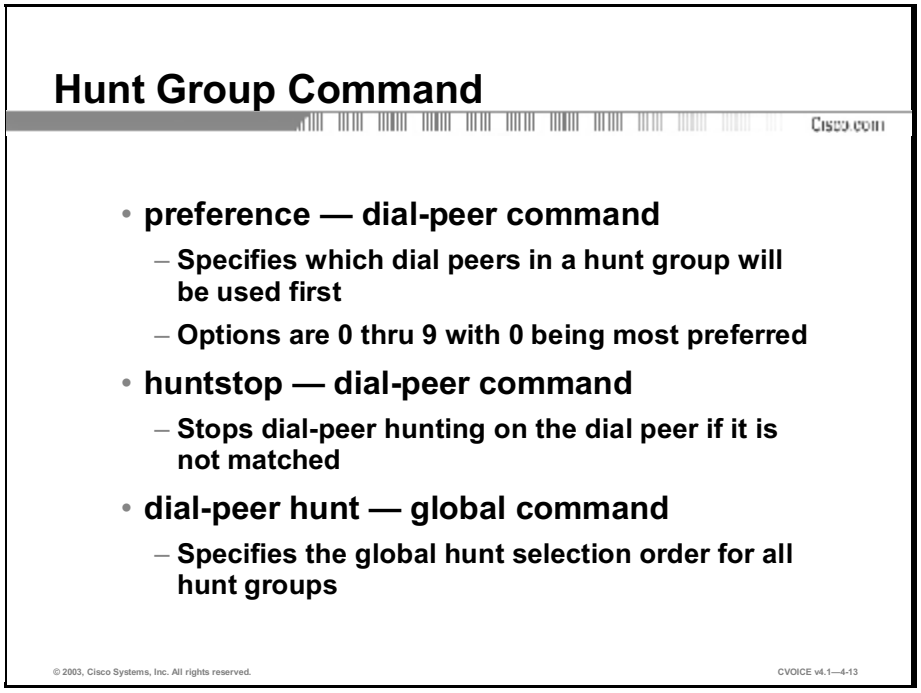
Step	Action
1	The router or gateway uses the dial peer **destination-pattern** command to determine how to route the call
2	The **destination-pattern** command routes the call in the following manner: ■ On POTS dial peers, the **port** command forwards the call ■ On VoIP dial peers, the **session target** 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

In the figure, dial-peer 1 matches any digit string that has not matched other dial peers more specifically. Dial-peer 2 matches any seven-digit number in the 2000 and 3000 range of numbers starting with 555. Dial-peer 3 matches any seven-digit number in the 1000 range of numbers starting with 555. Dial-peer 4 matches the specific number 5551234 only. When the number 5551234 is dialed, dial-peers 1, 3, and 4 all match that number, but dial-peer 4 places that call because it has the most specific destination pattern.

Hunt Group Commands

This topic describes hunt group commands.



The following is a list of hunt group commands:

- **preference:** Sets priority for dial peers. The destination with the lowest setting has the highest priority.
- **dial-peer hunt:** Changes the default selection order for hunting through dial peers.
- **show dial-peer voice summary:** Shows the current settings for dial-peer hunt.
- **huntstop:** Disables dial-peer hunting on the dial peer.

Configuring Hunt Groups

This topic describes how to configure hunt groups.

In some business environments, such as call centers or sales departments, there may be a group of agents available to answer calls coming into 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 to configure hunt groups:

Table 8: 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, then 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**, use the **show dial-peer voice summary** command.

If the desired action is not hunting through a range of dial peers, the **huntstop** command disables dial-peer hunting on the dial peer. 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. If this is not the desired action, then 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; however, if that network connectivity fails, you want to 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 following criteria, in the order listed:

Table 9: How the Router Selects Dial Peers in a Hunt Group

Step	Action
1	The router matches the most specific phone number
2	The router matches according to the preference setting
3	The router matches randomly

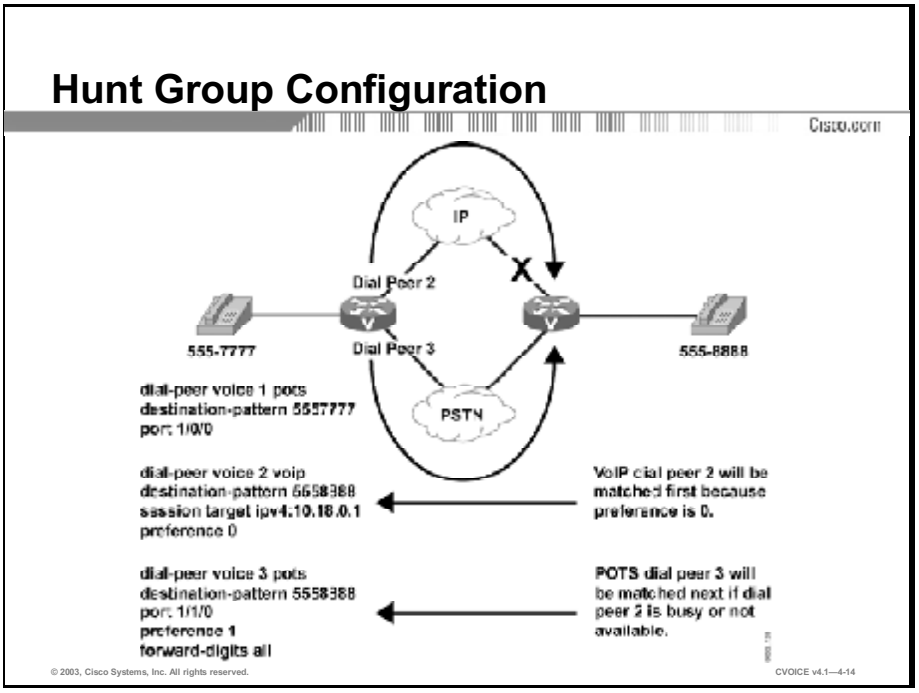
The destination pattern that matches the greatest number of dialed digits is the first dial peer selected by the router. For example, if one dial peer is configured with a dial string of “345….” and a second dial peer is configured with 3456789, the router selects 3456789 first because it has the longest 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 a secretary, 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. You would use the **preference** command to configure service for scenario 2, where the dial peers connecting to the senior agents would have the preference 0 and the dial peers connecting to the junior agents would have the preference 1. The lower the preference setting, the higher the priority for that dial peer to handle the call.

If all destination patterns are equal, by default, the preference is set to 0 on all dial peers. If the preference does not act as the tiebreaker, then a dial peer matching the called number will be picked randomly. This configuration would service scenario 1.

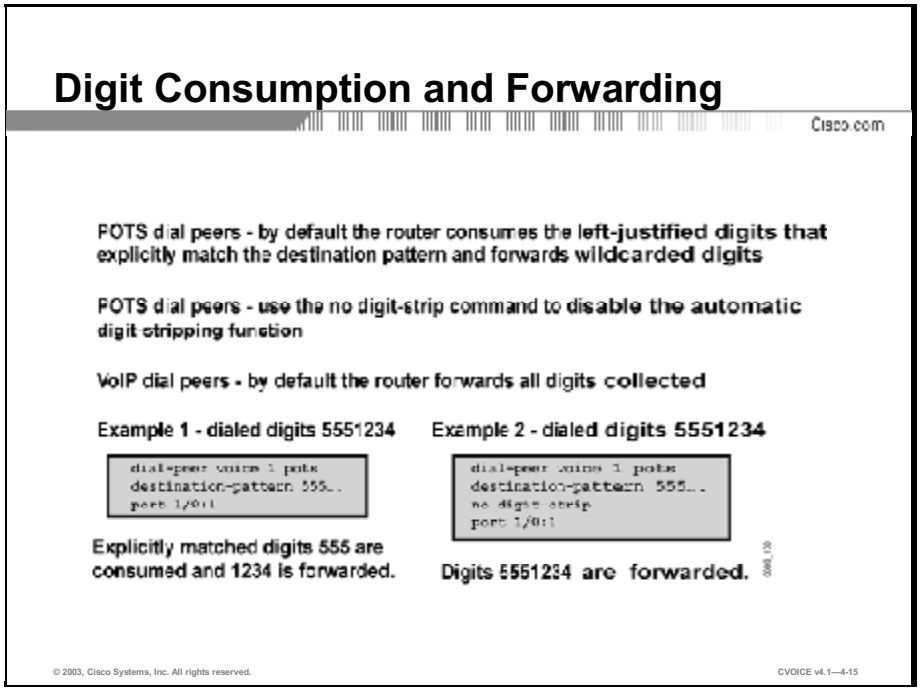
Example

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 555-8888, VoIP dial-peer 2 is matched first because the preference is set to zero. 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.



Digit Collection and Consumption

This topic describes how the router collects and consumes digits and applies them to the dial peer statements.

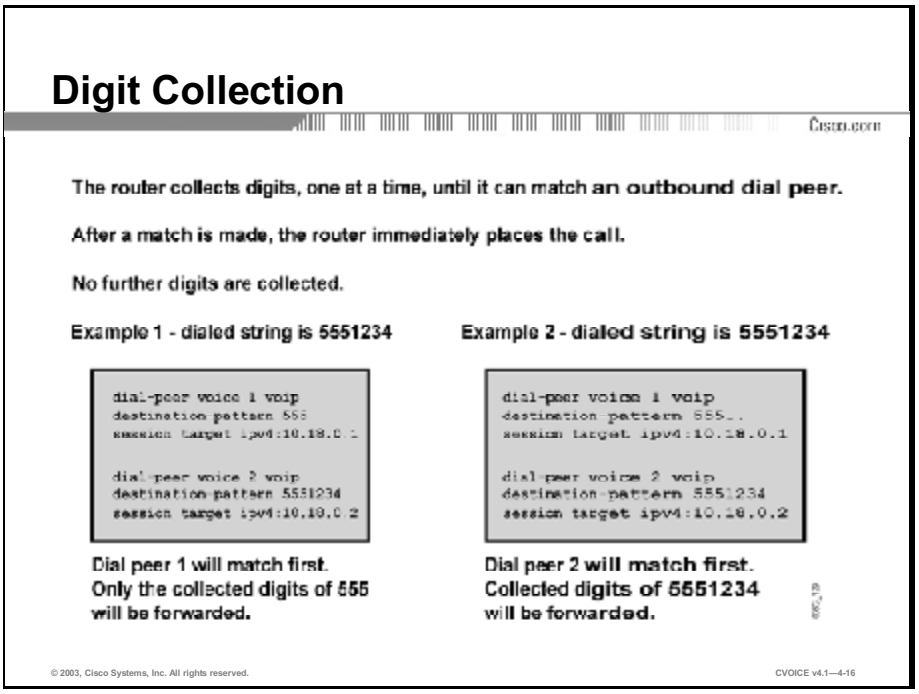


Use the **no digit-strip** command to disable the automatic digit-stripping function. This allows the router to match digits and pass them to the telephony interface.

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 digits, or *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 an FXS port that connects a telephone or fax machine. If digit stripping is turned off on this type of port, the user may hear tones after answering the call because any unconsumed and unmatched digits are passed through the voice path after the call is answered.

In other situations, where 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 this situation, 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.



When a voice call enters the network:

Table 10: 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

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. Because the router matches one digit at a time against available dial peers, 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.

Table 11: Matching Destination Patterns

Dialed Digits	Destination Pattern	Dialed Digits Collected
5551234	5……	5551234
5551234	555….	5551234
5551234	555	555
5551234	555T	5551234

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.

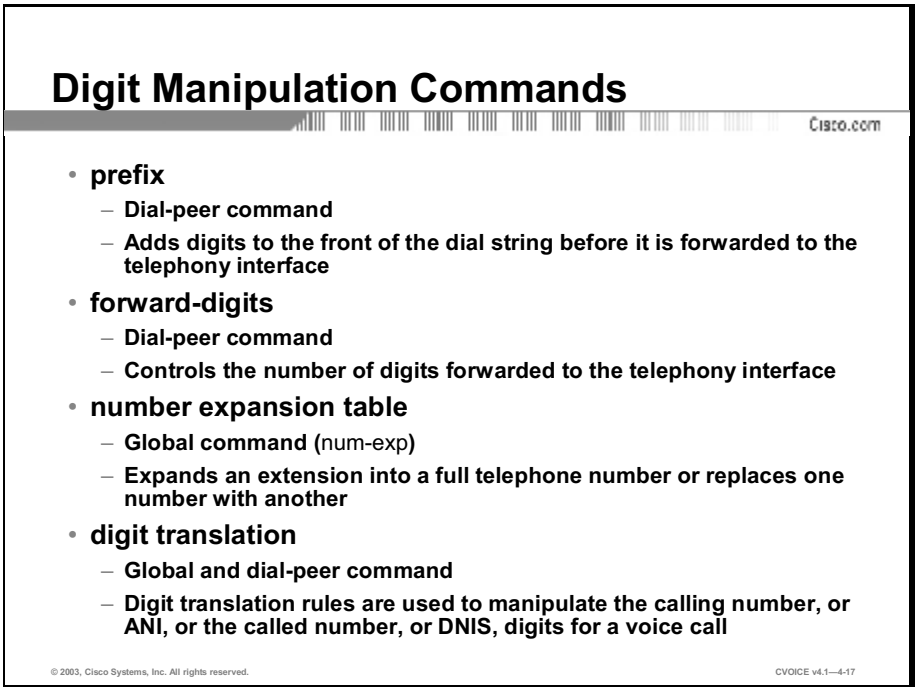
In the second row, the destination pattern specifies a seven-digit string. The first three digits must be 555, and the remaining four digits can be any valid digits. All seven digits must be entered before the destination pattern is matched.

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.

What Is Digit Manipulation?

This topic describes digit manipulation and the commands that are used to connect to a specified destination.



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. The following is a list of digit manipulation commands and their uses:

- **prefix:** This dial-peer 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 four-digit extension such as 1234, but the call needs to be routed to the PSTN, which requires ten digit dialing. If the four-digit extension matches the last four digits of the actual PSTN telephone number, then you can use the **prefix** command, **prefix 902555**, to prepend the six additional digits needed for the PSTN to route the call to 902-555-1234. After the POTS dial peer is matched with the destination pattern of 1234, the **prefix** command prepends the additional digits, and the string 9025551234 is sent out of the voice port to the PSTN.

- **forward-digits:** This dial-peer command specifies the number of digits that must be forwarded to the telephony interface, regardless of whether they are explicitly matched or wildcard matched. This command occurs after the outbound dial peer is matched, but before the digits are sent out of the telephony interface. When a specific number of digits are configured for forwarding, the count is right justified. For example, if 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.

Note	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.

- **number expansion table** (num-exp)**:** This 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 is useful, for example, where the PSTN changes the dialing requirements from seven-digit dialing to ten-digit dialing. In this scenario, you can do one of the following:
  - Make all the users dial all ten digits to match the new POTS dial peer that is pointing to the PSTN
  - Allow the users to continue dialing the seven-digit number as they have before, but expand the number to include the area code before the ten-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 *number*** command to confirm the presence off a valid dial peer to match the newly expanded number.

- **digit translation**: 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 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 five-digit extension into the ten-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. In many cases, several of these tools will provide a workable solution. 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

The following 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 of 555 before forwarding the four wildcard-matched digits.

The following 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.

The following is a sample configuration using the **number expansion table** command:

num-exp 2… 5552…

dial-peer voice 1 pots

destination-pattern 5552…

port 1/1/0

In the sample configuration using the **number expansion table** command, the extension number of 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.

The following is a sample configuration using the **digit translation** 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.

The following 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.....

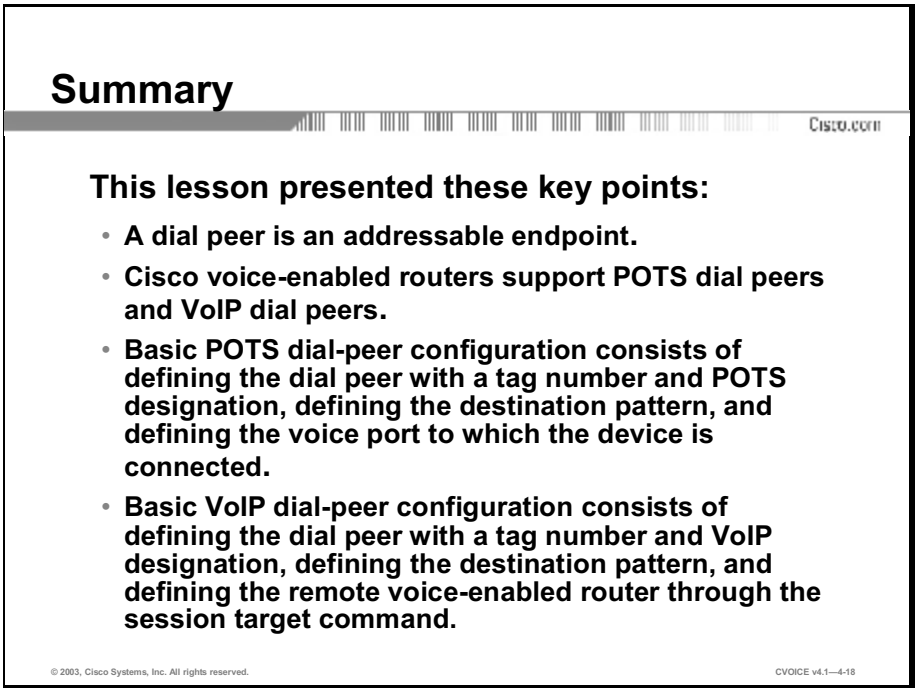
translate-outgoing called 20

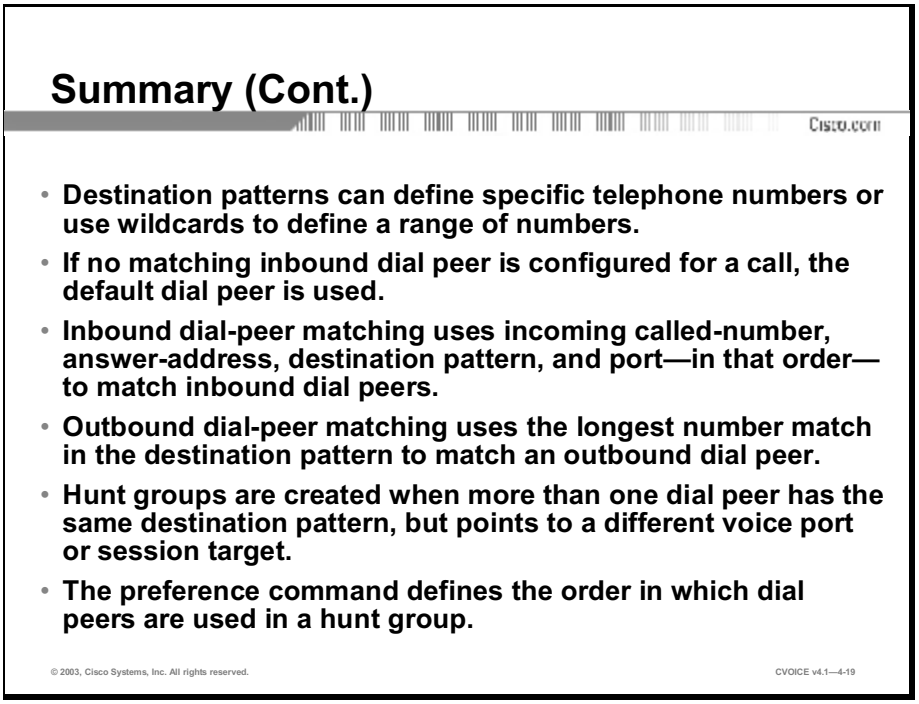
port 1/1:5

forward-digits all

Summary

This topic summarizes the key points discussed in this lesson.





Summary (Cont.)

- The hunt-stop 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.

Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Dial Peers
- Assessment (Complex Lab): Refer to Lab 4-1, contained in Laboratory Exercises in Additional Resources section E.
- Special-Purpose Connections lesson

References

For additional information, refer to these resources:

- "Dial Peer Overview"
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfpeers.htm#xtocid2

- "Case Study: Understanding Inbound Matching and Default Dial-Peer 0"
  http://www.cisco.com/warp/public/788/voip/in_dial_peer_match.html#fifth

- "Voice—Understanding Inbound and Outbound Dial Peers on Cisco IOS"
  http://www.cisco.com/warp/public/788/voip/in_out_dial_peers.html

- VR: Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_r/

- Cisco IP Telephony, Cisco Press; ISBN: 1587050501; 1st edition (December 17, 2001)

Quiz: Dial Peers

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe dial peers and their application
- Configure plain old telephone service dial peers
- Configure Voice over IP 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
- List hunt group commands
- Configure hunt groups
- Describe how the router and attached telephony equipment collect and consume digits, and apply them to the dial peer
- Describe digit manipulation and the commands that are used to connect to a specified destination

Instructions

Answer these questions:

Q1) 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

Q2) The address is configured on each dial peer and is called a _____.

A) telephone number

B) number range

C) destination pattern

D) call endpoint

Q3) 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

Q4) 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

Q5) 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**

Q6) What happens if a loopback address is 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) None of the above.

Q7) 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.

Q8) Which special character in a destination pattern string is used as a wildcard?

A) asterisk (*)

B) pound sign (#)

C) comma (,)

D) period (.)

E) brackets ([])

Q9) 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) None of the above.

Q10) What is the default dial-peer configuration for inbound POTS peers?

A) any codec

B) no ivr application

C) vad enabled

D) no rsvp support

E) ip precedence 0

Q11) Which configurable parameter is set for POTS dial peers only?

A) answer-address

B) destination-pattern

C) incoming called-number

D) port

Q12) 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

Q13) Write the number of the dial peer configuration in the space beside the specified destination to which it is matched first.

1. dial-peer voice 1 pots
   destination-pattern .T
   port 1/0:1

2. dial-peer voice 2 pots
   destination-pattern 555[0-2,5]…
   port 1/1/0

3. dial-peer voice 1 pots
   destination-pattern 5553…
   port 1/0:1

4. dial-peer voice 1 pots
   destination-pattern 5553216
   port 1/0.1

_____ 1. dialed number is 5551234

_____ 2. dialed number is 5550000

_____ 3. dialed number is 567-1234

_____ 4. dialed number is 5553216

_____ 5. dialed number is 5553000

_____ 6. dialed number is 555000

Q14) When the router is matching 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*

Q15) 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

Q16) 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
```

Q17) By default, which 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.

Q18) 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**

Q19) The user is dialing the number 5551234. 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 5551234
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
```

_____

Q20) What is the default behavior of a terminating router when it is matching a dial string to an outbound POTS dial peer?

A) The router removes the left-most 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.

Q21) A **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

Q22) When 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

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Special-Purpose Connections

Overview

This lesson explores the uses and applications of various special-purpose connections on Cisco Systems telephony equipment.

Importance

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 off the PBX, regardless of where they 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:

- Identify different special-purpose connection types
- Describe how the network establishes private line, automatic ringdown and private line, automatic ringdown Off-Premises eXtension connections
- Configure trunk connections
- Describe how the network establishes tie-line connections

Learner Skills and Knowledge

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

- Familiarity with trunk and tie-line concepts
- Familiarity with voice port configuration

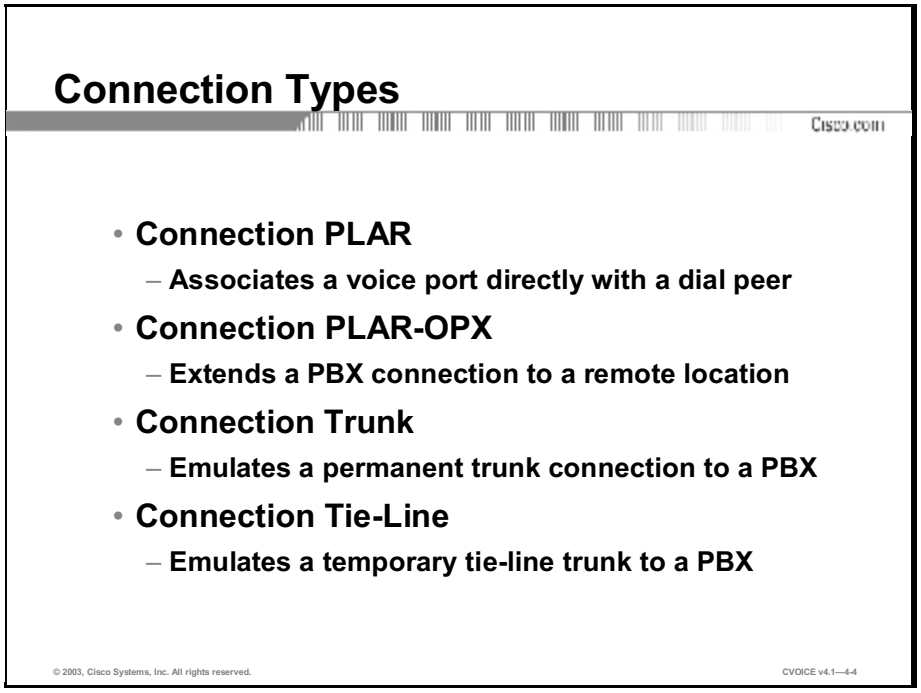
Outline

This lesson includes these topics:

- Overview
- Connection Types
- PLAR and PLAR OPX
- Configuring Trunk Connections
- Tie-Line Connections
- Summary
- Assessment (Quiz): Special-Purpose Connections
- Assessment (Complex Lab): Lab Exercise 4-2

Connection Types

This topic identifies different special-purpose connection types.



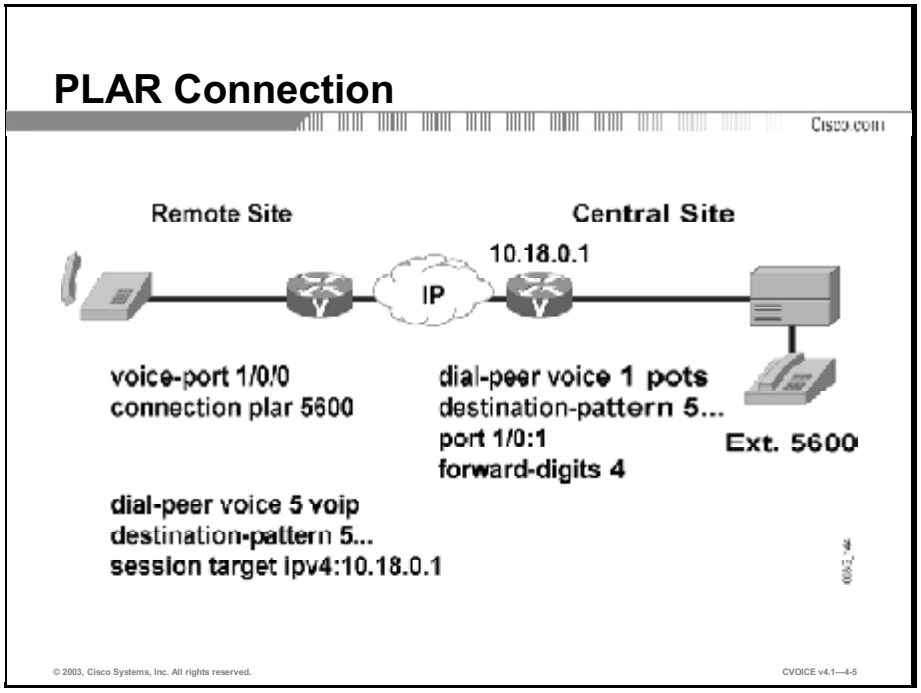
You can configure voice ports to support special connection requirements. These requirements usually reflect the needs of a specific business environment that must connect to the network in a special way. The following is a list of available connection types and their application:

- **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 pad.

- **PLAR Off-Premises eXtension (plar-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 on-site staff 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, on-site 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 Call Manager will not report a call completion until the far end has answered the call. Without the OPX configuration, the PBX or Cisco Call Manager passes the call to the local gateway and/or router. Then, the gateway and/or router routes the call to the public switched telephone network (PSTN). After the PSTN sends ringing to the telephone, the router will report call completion back to the PBX or Cisco Call Manager. At this point, the call is considered completed, and in fact it is. 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 Call Manager perspective, the call is completed. When you configure the OPX however, the gateway and/or router will not report call completion unless the telephone is actually answered.
- **Connection trunk:** 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 re-establishes 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 and/or router. Because this is a permanent connection, digit manipulation is not necessary.
- **Connection tie-line:** 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, then the digits that are sent to be matched against the outbound dial peer would be 78000. This new 5-digit number would be carried across the network to the remote site. At the remote route, the number 7 can be stripped off or, if necessary, passed to the destination device.

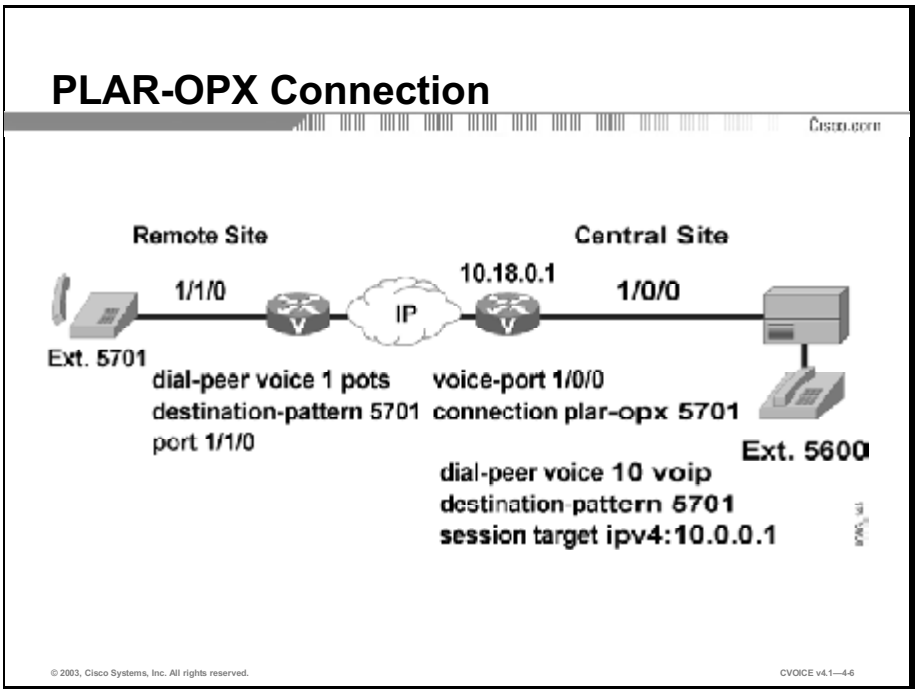
PLAR and PLAR OPX

This topic describes the use of PLAR and plar-opx connections.



As demonstrated in the figure, the following 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 Voice over IP (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, it sends a call-complete setup 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.

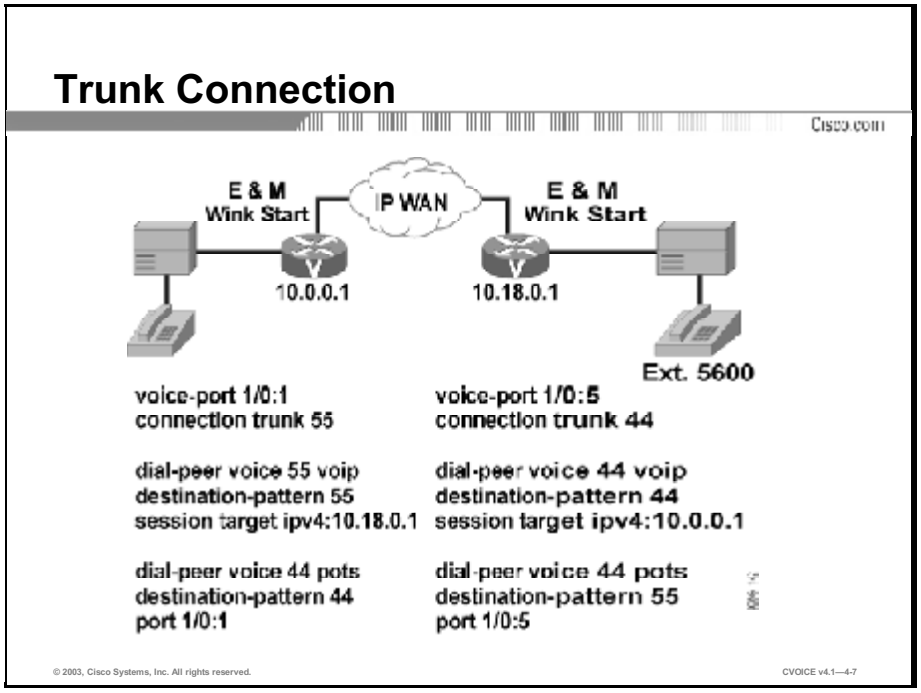


As demonstrated in the figure, the following actions must occur to establish a plar-opx connection:

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 and/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 PBX and opens a voice path.

Configuring Trunk Connections

This topic describes how to configure trunk connections.



As demonstrated in the figure, the following must occur 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 for each IP address.

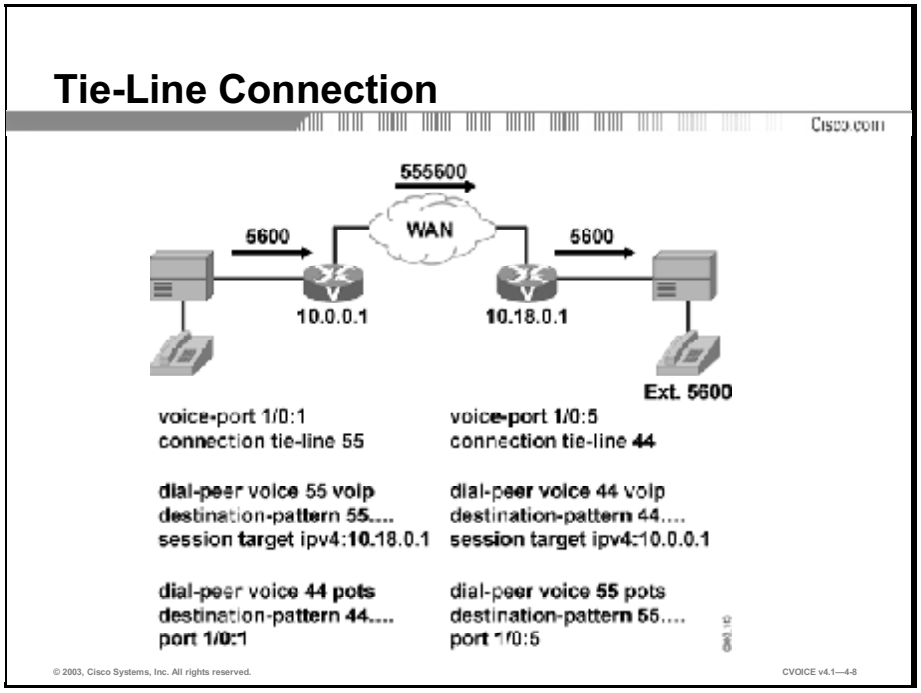
In the example, the router on the left is configured to set up a trunk connection from voice port 1/0:1 to a remote voice-enabled router with the IP address of 10.18.0.1 (the router on the right). This is done by specifying the same number in the **connection trunk** voice port command as in the appropriate dial peer **destination-pattern** command. 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). 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.

The following conditions must be met for VoIP to support virtual trunk connections:

- You must use the following voice port combinations:
  - recEive and transMit or ear and mouth (E&M) to E&M (same type)
  - Foreign Exchange Station (FXS) to Foreign Exchange Office (FXO)
  - FXS to FXS (with no signaling)
- Do not perform number expansion on the destination-pattern telephone numbers configured for trunk connection.
- You must configure both end routers for trunk connections.

Tie-Line Connections

This topic describes the use and application 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.

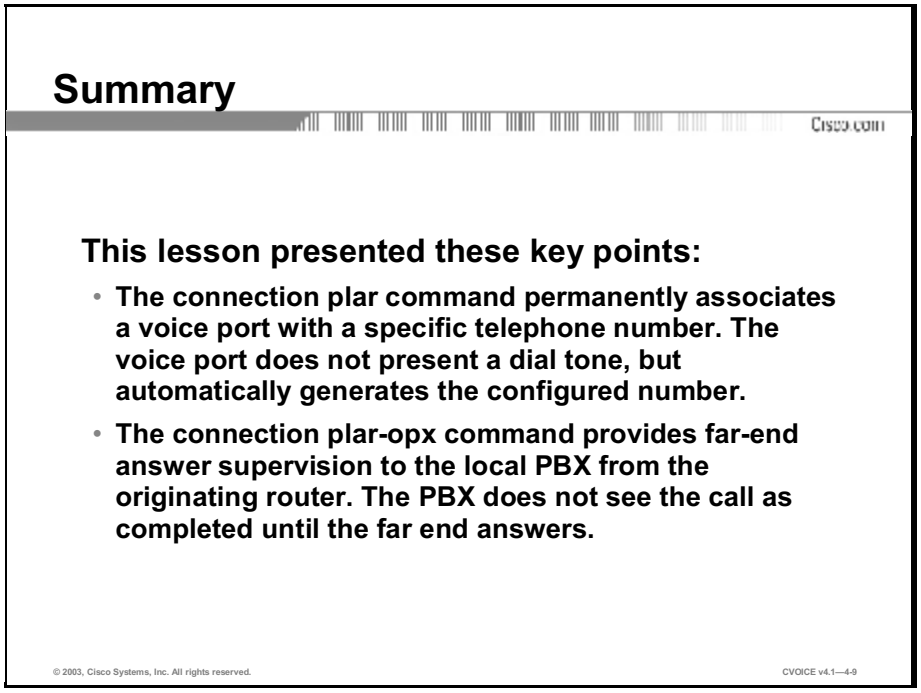
As demonstrated in the figure, you must complete the following procedure to establish a tie-line connection:

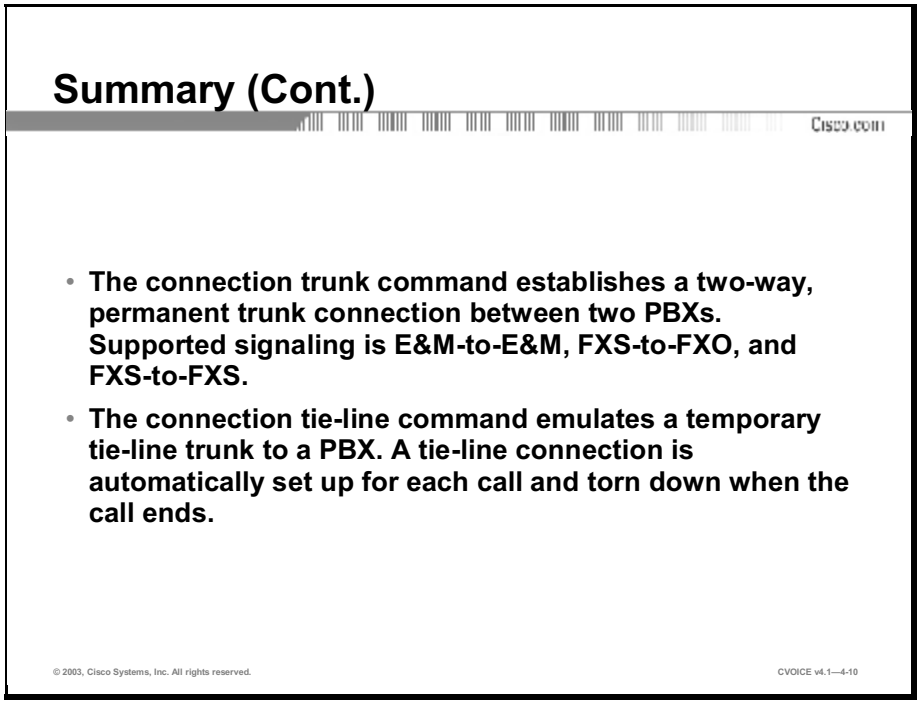
1. Use the **connection tie-line** command when the dial plan requires the addition of digits in front of any digits dialed by the PBX.
2. Use the combined set of digits to route the call onto the network.
3. The tie-line port waits to collect digits from the PBX.
4. The terminating router automatically 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 **connection tie-line**, the router collects the four digits and prepends the tie-line digits “55” to make them 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 of “55….”. Because POTS dial peers, by default, forward only wild card digits, only the four-digit extension of 5600 is passed to the PBX.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Special-Purpose Connections
- Assessment (Complex Lab): Refer to Lab 4-2, contained in Laboratory Exercises in Additional Resources section E.
- Introduction to Voice over IP module

References

For additional information, refer to these resources:

- "Cisco IOS Voice, Video, and Fax Command Reference" http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tvr/tvrc/vrg_c4.htm#xtocid7

Quiz: Special-Purpose Connections

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Identify different special-purpose connection types
- Describe how the network establishes private line, automatic ringdown and private line, automatic ringdown Off-Premises eXtension connections
- Configure trunk connections
- Describe how the network establishes tie-line connections

Instructions

Answer these questions:

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** parameter 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

E) all of the above

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.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

5

Introduction to Voice over IP

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, bandwidth requirements using different coder-decoders (codecs) and data links, and implementing solutions. The role of gateways and their use in integrating VoIP with traditional voice technologies is explained. Other voice over network technologies such as Frame Relay and ATM are discussed and compared to VoIP.

Upon completing this module, you will be able to:

- Determine the best method to improve delivery of voice packets with minimal loss, delay, or jitter, given the challenges associated with implementing VoIP solutions
- Discuss the challenges associated with voice delivery in IP, Frame Relay, or ATM networks, when provided the differences and similarities among VoIP, Voice over Frame Relay and Voice over ATM
- Select the correct gateway for an enterprise and service provider network, given the definition of gateways and their role within a network
- Reduce header size to efficiently carry voice across the network, using the VoIP protocols and compressed Real-Time Transport Protocol
- List the bandwidth requirements for various codecs and data links, and the methods to reduce bandwidth consumption, given the formula to calculate total bandwidth for a VoIP call
- Describe the implications of implementing security measures in IP networks that will transport voice, when provided with the elements of a security policy

Outline

The module contains these lessons:

- Requirements of Voice in an IP Internetwork
- VoIP vs. Voice over Frame Relay or Voice over ATM
- Gateways and Their Roles
- Encapsulating Voice in IP Packets
- Bandwidth Requirements
- Security Implications

Requirements of Voice in an IP Internetwork

Overview

This lesson describes the fundamentals of Voice over IP (VoIP) and identifies the challenges and solutions regarding its implementation.

Importance

To implement VoIP solutions, you must understand how IP networks operate and what impact they have on voice traffic. Packet loss, delay, and jitter are some of the challenges voice encounters in an IP environment. This lesson will highlight these issues and discuss methods to deal with them.

Objectives

Upon completing this lesson, you will be able to:

- Explain which characteristics of IP networks cause problems for real-time traffic
- Describe packet loss, delay, and jitter problems in IP networks and identify a solution for each problem
- Describe five techniques that are used by Cisco IOS® software to ensure consistent delivery and throughput of voice packets in an IP network
- Illustrate the steps used by the Real-Time Transport Protocol to reorder packets on IP networks
- Describe four methods for improving reliability and availability of the IP internetwork for the delivery of voice packets

Learner Skills and Knowledge

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

- Familiarity with IP network concepts dealing with reliability, throughput, delay, and loss

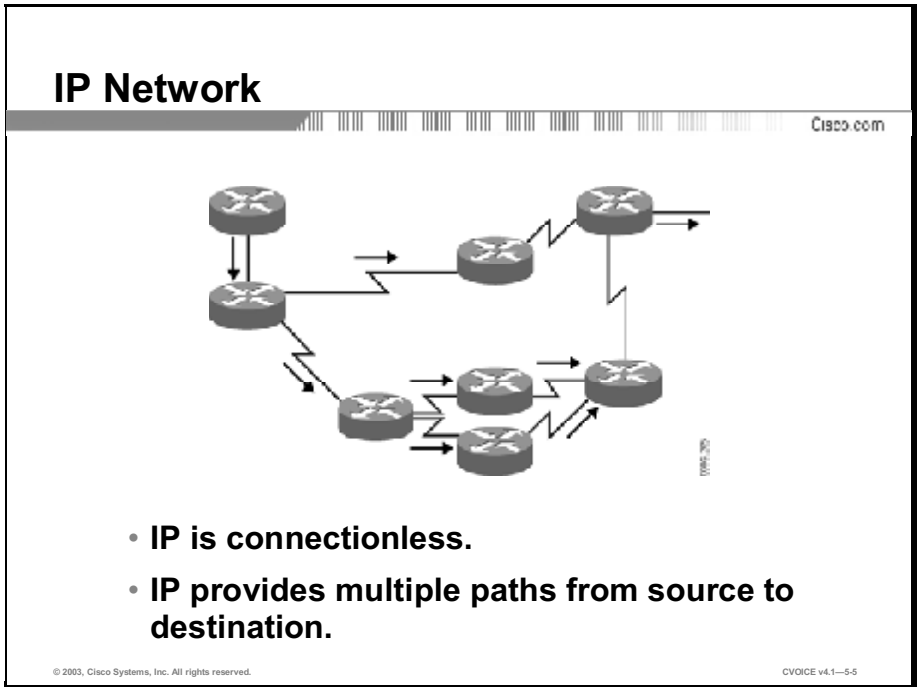
Outline

This lesson includes these topics:

- Overview
- Real-Time Voice in a Best-Effort IP Internetwork
- Packet Loss, Delay, and Jitter
- Consistent Throughput
- Reordering of Voice Packets
- Reliability and Availability
- Summary
- Assessment (Quiz): Requirements of Voice in an IP Internetwork

Real-Time Voice in a Best-Effort IP Internetwork

This topic lists problems associated with implementation of real-time voice traffic in a best-effort IP internetwork.



The traditional telephony network was originally designed to carry voice. The design of circuit-switched calls provides a guaranteed path and delay threshold between source and destination. The IP network was originally designed to carry data. Data networks were not designed to carry voice traffic. Although data traffic is best-effort traffic and can withstand some amount of delay, jitter, and loss, voice traffic is real-time traffic that requires a certain quality of service (QoS). In the absence of any special QoS parameters, a voice packet is treated as just another data packet.

The user must have a well-engineered network, end to end, when running delay-sensitive applications such as Voice over IP (VoIP). Fine-tuning the network to adequately support VoIP involves a series of protocols and features geared toward QoS.

Example

In the IP network shown in the figure, voice packets that enter the network at a constant rate can reach the intended destination by a number of routes. Because each of these routes may have different delay characteristics, the arrival rate of the packets may vary. This condition is called jitter.

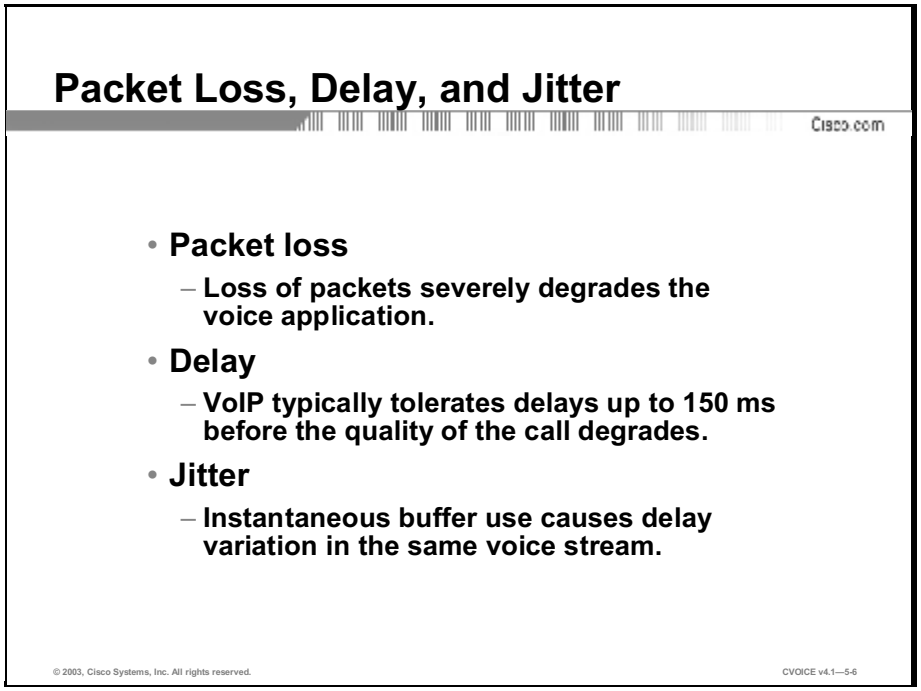
Another effect of multiple routes is that voice packets can arrive out of order. The far-end voice-enabled router or gateway has to resort the packets and adjust the interpacket interval for a proper-sounding voice playout.

Network transmission adds corruptive effects like noise, delay, echo, jitter, and packet loss to the speech signal. VoIP is susceptible to these network behaviors, which can degrade the voice application.

If a VoIP network is to provide the same quality that users have come to expect from traditional telephony services, then the network must ensure that the delay in transmitting a voice packet across the network, and the associated jitter, does not exceed specific thresholds.

Packet Loss, Delay, and Jitter

This topic discusses the causes of packet loss, end-to-end delay, and jitter delay in an IP internetwork.



In traditional telephony networks, voice has a guaranteed delay across the network through strict bandwidth association with each voice stream. Configuring voice in a data network environment requires network services with low delay, minimal jitter, and packet loss. Over the long term, delay, jitter, and packet loss will all affect overall voice quality. Voice quality problems include:

- **Packet loss:** You can drop voice packets if the network quality is poor, if the network is congested, or if there is too much variable delay in the network. Coder-decoder (codec) algorithms can correct small amounts of loss but too much loss can cause voice clipping and skips. The chief cause of packet loss is network congestion.

- **Delay:** End-to-end delay is the time that it takes the sending endpoint to send the packet to the receiving endpoint. End-to-end delay consists of the following two components:

  – **Fixed network delay:** You should examine fixed network delay during the initial design of the VoIP network. The International Telecommunications Union (ITU) standard G.114 states that a one-way delay budget of 150 ms is acceptable for high-quality voice. Research at Cisco Systems has shown that there is a negligible difference in voice quality scores using networks built with 200-ms delay budgets. Examples of fixed network delay include propagation delay of signals between the sending and receiving endpoints, voice encoding delay, and voice packetization time for various VoIP codecs.

- **Variable network delay:** Congested egress queues and serialization delays on network interfaces can cause variable packet delays. Serialization delay is a constant function of link speed and packet size. The larger the packet and the slower the link-clocking speed, the greater the serialization delay. Although this ratio is known, it can be considered variable because a larger data packet can enter the egress queue at any time before a voice packet. If the voice packet must wait for the data packet to serialize, the delay incurred by the voice packet is its own serialization delay, plus the serialization delay of the data packet in front of it.

- **Jitter:** Jitter is the variation between the expected arrival of a packet and when it is actually received. To compensate for these delay variations between voice packets in a conversation, VoIP endpoints use jitter buffers to turn the delay variations into a constant value so that voice can be played out smoothly. Buffers can fill instantaneously, however, because network congestion can be encountered at any time within a network. This instantaneous buffer use can lead to a difference in delay times between packets in the same voice stream.

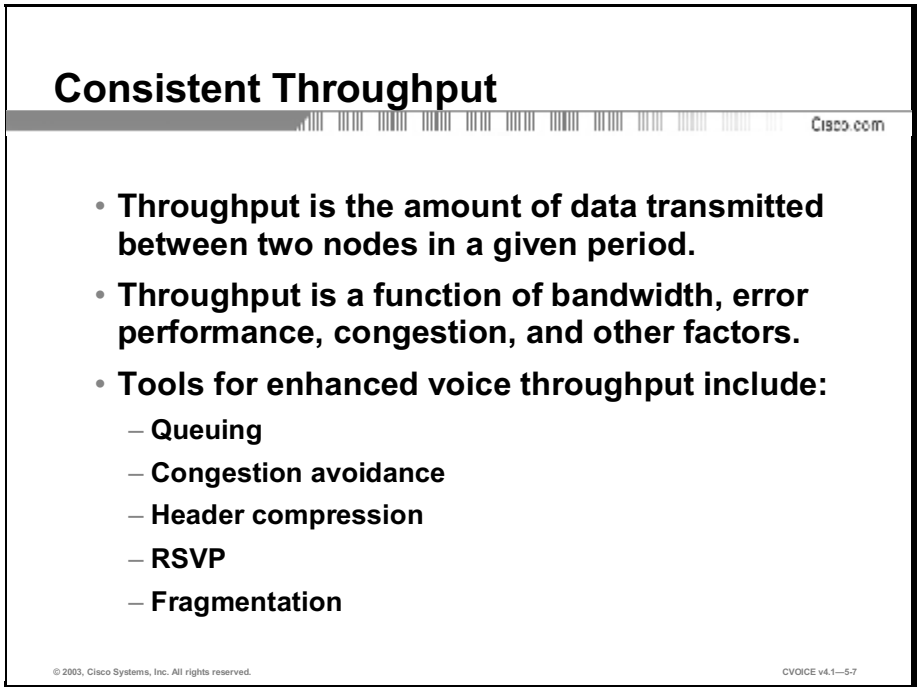
Example

The effect of packet loss, end-to-end delay, and jitter can be heard as follows:

- The calling party says, “Good morning, how are you?”
- With packet loss, the called party hears, “Good m..ning, w are you?”
- With end-to-end delay, the called party hears, “……Good morning, how are you?”
- With jitter, the called party hears, “Good……morning, how……are you?”

Consistent Throughput

This topic describes the methods you can use to ensure consistent delivery and throughput of voice packets in an IP internetwork.



Throughput is the actual amount of useful data that is transmitted from a source to a destination. The amount of data that is placed in the pipe at the originating end is *not* necessarily the same amount of data that comes out at the destination. The data stream may be affected by error conditions in the network; for example, bits may be corrupted in transit, leaving the packet unusable. Packets may also be dropped during times of congestion, potentially forcing a retransmit, using twice the amount of bandwidth for that packet.

In the traditional telephony network, voice had guaranteed bandwidth associated with each voice stream. Cisco IOS® software uses a number of techniques to reliably deliver real-time voice traffic across the modern data network. These techniques, which all work together to ensure consistent delivery and throughput of voice packets, include:

- **Queuing:** The act of holding packets so that they can be handled with a specific priority when leaving the router interface. Queuing enables routers and switches to handle bursts of traffic, measure network congestion, prioritize traffic, and allocate bandwidth. Cisco routers offer several different queuing mechanisms that can be implemented based on traffic requirements. Low Latency Queuing (LLQ) is one of the newest Cisco queuing mechanisms.

- **Congestion avoidance:** Congestion avoidance techniques monitor network traffic loads. The aim is to anticipate and avoid congestion at common network and internetwork bottlenecks *before* it becomes a problem. These techniques provide preferential treatment under congestion situations for premium (priority) class traffic, such as voice. At the same time, these techniques maximize network throughput and capacity use and minimize packet loss and delay. Weighted random early detection (WRED) is one of the QoS congestion avoidance mechanisms used in Cisco IOS software.

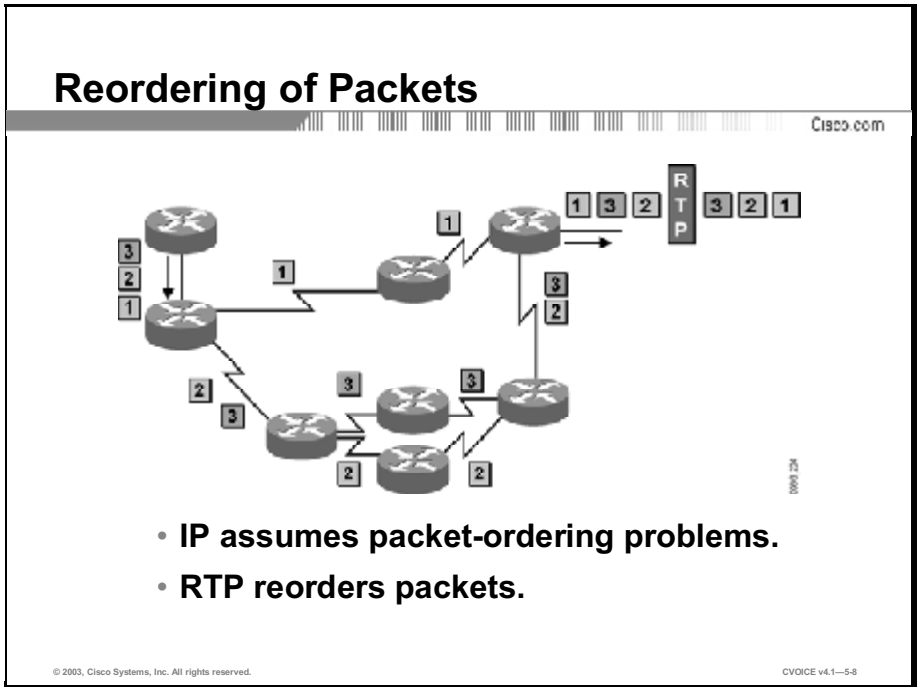
- **Header compression:** In the IP environment, voice is carried in Real-Time Transport Protocol (RTP), which is carried in User Datagram Protocol (UDP), which is then put inside an IP packet. This constitutes 40 bytes of RTP/UDP/IP header. This header size is large when compared to the typical voice payload of 20 bytes. Compressed RTP (CRTP) reduces the headers to 2 bytes in most cases, thus saving considerable bandwidth and providing for better throughput.

- **Resource Reservation Protocol:** Resource Reservation Protocol (RSVP) is a transport layer protocol that enables a network to provide differentiated levels of service to specific flows of data. Unlike routing protocols, RSVP is designed to manage flows of data rather than make decisions for each individual datagram. Data flows consist of discrete sessions between specific source and destination machines. Hosts use RSVP to request a QoS level from the network on behalf of an application data stream. Routers use RSVP to deliver QoS requests to other routers along the paths of the data stream. After an RSVP reservation is made, weighted fair queuing (WFQ) is the mechanism that actually delivers the queue space at each device. Voice calls in the IP environment can request RSVP service to provide guaranteed bandwidth for a voice call in a congested environment.

- **Fragmentation:** Fragmentation defines the maximum size for a data packet and is used in the voice environment to prevent excessive serialization delays. Serialization delay is the time that it takes to actually place the bits onto an interface. For example, a 1500-byte packet takes 187 ms to leave the router over a 64-kbps link. If a best-effort data packet of 1500 bytes is sent, real-time voice packets are queued until the large data packet is transmitted. This delay is unacceptable for voice traffic. However, if best-effort data packets are fragmented into smaller frames pieces, they can be interleaved with real-time (voice) packets. In this way, both voice and data packets can be carried together on low-speed links *without* causing excessive delay to the real-time voice traffic.

Reordering of Voice Packets

This topic describes how RTP ensures consistent delivery order of voice packets in an IP internetwork.



In traditional telephony networks, voice samples are carried in an orderly manner through the use of time-division multiplexing (TDM). Because the path is circuit-switched, the path between the source and destination is reserved for the duration of the call. All of the voice samples stay in order as they are transmitted across the wire. Because IP provides connectionless transport with the possibility of multiple paths between sites, voice packets cannot arrive out of order at the destination. Because voice rides in UDP/IP packets, there is no automatic reordering of packets.

RTP provides end-to-end delivery services for data that requires real-time support, such as interactive voice and video. According to RFC 1889, the services provided by RTP include payload-type identification, sequence numbering, time stamping, and delivery monitoring.

Example

In the figure here, RTP reorders the voice packets through the use of sequence numbers *before* playing them out to the user.

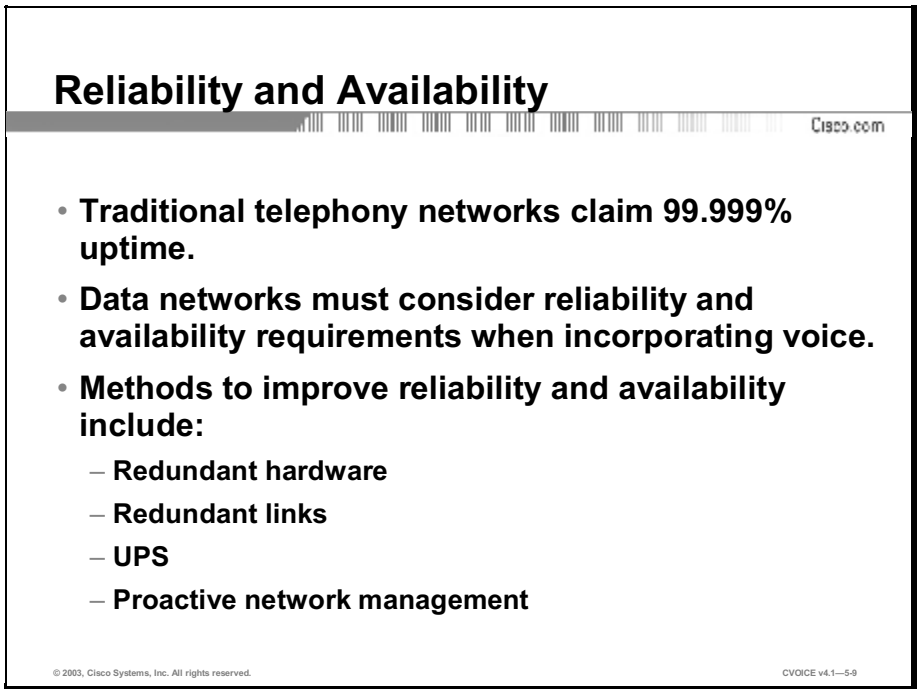
The table illustrates the various stages of packet reordering by RTP.

Table 1: Sequencing of Packets by RTP

Stage	What Happens
Voice packets enter the network.	IP assumes packet-ordering problems.
RTP reorders the voice packets.	The voice packets are put in order through the use of sequence numbers.
RTP retimes the voice packets.	The voice packets are spaced according to the time stamp contained in each RTP header.
	The user hears the voice packets in order and with the same timing as when the voice stream left the source.
RTCP (Real-time Transport Control Protocol) sends occasional report packet for delivery monitoring.	Both the sender and receiver send occasional report packets containing information, such as number of packets sent or received, the octet count, and the number of lost packets.

Reliability and Availability

The traditional telephony network strives to provide 99.99 percent uptime to the user. This corresponds to 5.25 minutes per year of down time. Many data networks cannot make the same claim. This topic describes methods that you can use to improve reliability and availability in data networks.



To provide telephony users the same—or close to the same—level of service as they experience with traditional telephony, the reliability and availability of the data network takes on new importance.

When the data network goes down, it may not come back up for minutes or even hours. This delay is unacceptable for telephony users. Local users, with network equipment such as voice-enabled routers, gateways, or switches for IP Phones, now find that their connectivity is terminated. Administrators must, therefore, provide an uninterruptible power supply (UPS) to these devices *in addition* to providing network availability. Previously, depending on the type of connection the user had, they received their power directly from the telephone company central office (CO) or through a UPS that was connected to their keyswitch or PBX in the event of a power outage. Now the network devices must have protected power to continue to function and provide power to the end devices.

Network reliability comes from incorporating redundancy into the network design. In traditional telephony, switches have multiple redundant connections to other switches. If either a link or a switch becomes unavailable, the telephone company can route the call in different ways. This is why telephone companies can claim a high availability rate.

High availability encompasses many areas of the network. In a fully redundant network, the following components need to be duplicated:

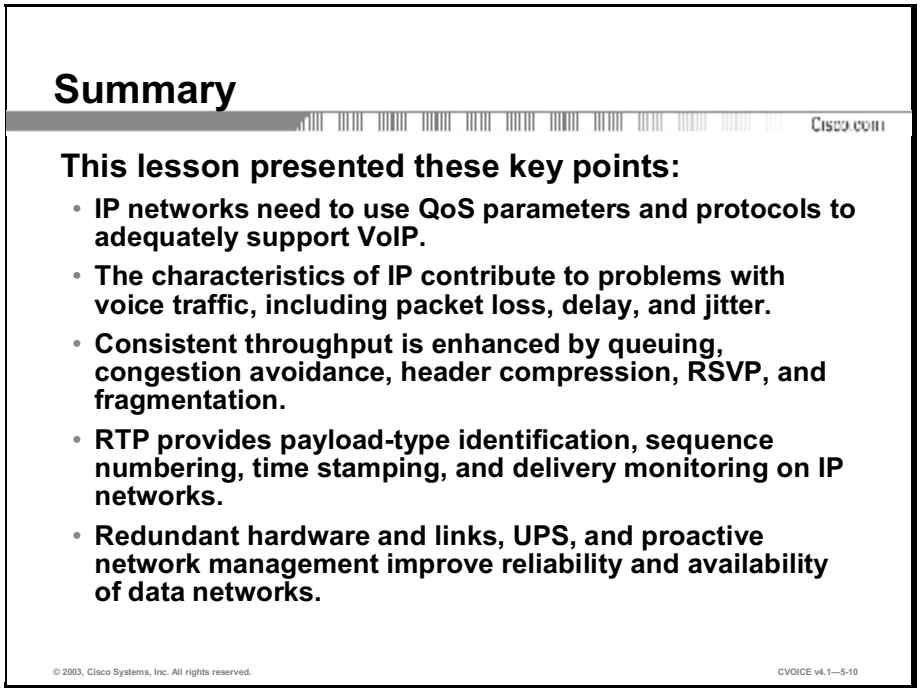
- Servers and call managers
- Access layer devices, such as LAN switches
- Distribution layer devices, such as routers or multilayer switches
- Core layer devices, such as multilayer switches
- Interconnections, such as WAN links, even through different providers
- Power supplies and UPSs

In some data networks, a high level of availability and reliability is not critical enough to warrant financing the hardware and links required to provide complete redundancy. If voice is layered onto the network, these requirements need to be revisited.

With Cisco Architecture for Voice, Video and Integrated Data (AVVID) technology, the use of Cisco CallManager clusters provides a way to design redundant hardware in the event of Cisco CallManager failure. When using gatekeepers, you can configure backup devices as secondary gatekeepers in case the primary gatekeeper fails. You must also revisit the network infrastructure. Redundant devices and Cisco IOS services, like Hot Standby Router Protocol (HSRP), can provide high availability. For proactive network monitoring and trouble reporting, a network management platform such as CiscoWorks2000 provides a high degree of responsiveness to network issues.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Requirements of Voice in an IP Internetwork
- VoIP vs. Voice over Frame Relay or Voice over ATM lesson

Quiz: Requirements of Voice in an IP Internetwork

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Explain which characteristics of IP networks cause problems for real-time traffic
- Describe packet loss, delay, and jitter problems in IP networks and identify a solution for each problem
- Describe five techniques that are used by Cisco IOS® software to ensure consistent delivery and throughput of voice packets in an IP network
- Illustrate the steps used by the Real-Time Transport Protocol to reorder packets on IP networks
- Describe four methods for improving reliability and availability of the IP internetwork for the delivery of voice packets

Instructions

Answer these questions:

Q1) What is one cause of jitter when voice packets are transmitted over an IP network?

A) congestion leading to instantaneous buffer utilization

B) the corruptive effect of noise

C) the loss of some voice packets on high-traffic lines

D) use of the PSTN

Q2) How can you ensure proper delivery of voice packets over an IP network?

A) by using QoS parameters

B) by using Frame Relay as the Layer-2 technology

C) by using circuit-switched paths only

D) by using high-speed links

Q3) According to ITU G.114, what is the maximum delay that VoIP can tolerate before voice quality starts to degrade?

A) 120 ms

B) 150 ms

C) 200 ms

D) 250 ms

Q4) What two conditions can result in voice packets being dropped during transmission across an IP network? (Choose two.)

A) The network quality is poor.

B) There is too much variable delay in the network.

C) The router is down.

D) The switch handles data packets only.

Q5) Match the Cisco IOS tools for enhanced voice throughput with their description.

A) queuing

B) congestion avoidance

C) header compression

D) RSVP

E) fragmentation

_____ 1. provides preferential treatment for priority traffic

_____ 2. holds packets so that they can be handled with a specific priority when they leave the router interface

_____ 3. defines the maximum size of a data packet

_____ 4. enables the network to provide differentiated levels of service to specific flows of data

_____ 5. saves bandwidth by compressing the header

Q6) Which technique is used to prevent excessive serialization delay?

A) queuing

B) congestion avoidance

C) header compression

D) RSVP

E) fragmentation

Q7) Which protocol automatically reorders packets?

A) TDM

B) IP

C) UDP

D) RTP

Q8) What is the function of RTCP in ensuring consistent delivery of voice packets in an IP network?

A) reorders the voice packets through the use of sequence numbers

B) retimes the voice packets based on time stamps

C) sends occasional report packets for delivery monitoring

D) all of the above

Q9) Which Cisco technology can be used to provide proactive network management?

A) Cisco IOS services

B) Cisco AVVID

C) Cisco CallManager

D) CiscoWorks2000

Q10) What do traditional telephony networks typically use to provide redundancy?

A) multiple servers

B) multilayer switches

C) multiple connections between switches

D) all of the above

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Voice over IP vs. Voice over Frame Relay or Voice over ATM

Overview

This lesson provides a comparison between Voice over IP (VoIP) technology and other voice transport technologies. The purpose of the comparison is to introduce other voice-related transport technologies and examine the various challenges associated with voice delivery.

Importance

Network administrators must realize that there are other transport technologies for voice. A basic understanding of these technologies and the challenges that each of them present, will help you develop a better understanding of VoIP.

Objectives

Upon completing this lesson, you will be able to:

- Compare single-path and multiple-path networks and list at least one advantage and disadvantage for each type of network
- Describe how voice packets are recognized by TCP/IP, Frame Relay, and ATM for preferential management by the technology
- Describe the functions of the Frame Relay Forum standard 11 fields that are used to encapsulate voice packets in Voice over Frame Relay
- List three variables that affect bandwidth in Voice over Frame Relay and use a formula to calculate the required bandwidth

- Describe the method of voice encapsulation that is used in Voice over ATM and provide two examples
- List five variables that affect bandwidth in Voice over ATM and use a formula to calculate the required bandwidth

Learner Skills and Knowledge

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

- Knowledge of TCP/IP networks
- Basic knowledge of traditional telephony networks
- Knowledge of real-time versus not real-time traffic delivery problems

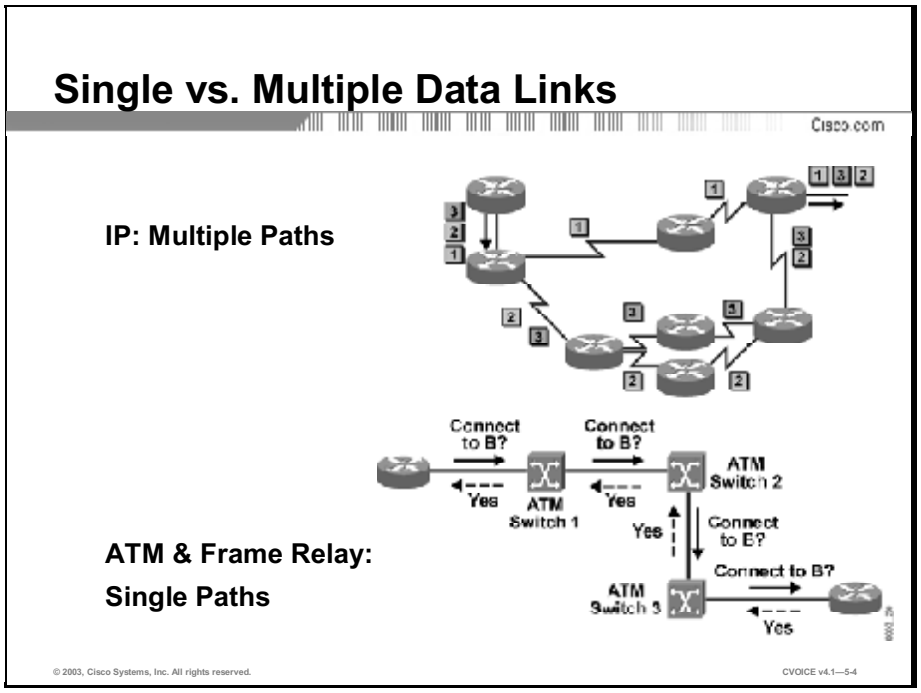
Outline

This lesson includes these topics:

- Overview
- Single vs. Multiple Data Links in the Call Path
- Recognizing Voice Packets in a Stream of Voice and Data
- Voice over Frame Relay Encapsulation
- Calculating Voice over Frame Relay Bandwidth
- Voice over ATM Encapsulation
- Calculating Voice over ATM Bandwidth
- Summary
- Assessment (Quiz): Voice over IP vs. Voice over Frame Relay or Voice over ATM
- Assessment (Complex Lab): Lab Exercise 5-1

Single Versus Multiple Data Links in the Call Path

This topic compares the paths that are used by protocol data units (PDUs) over IP networks and ATM and Frame Relay networks.

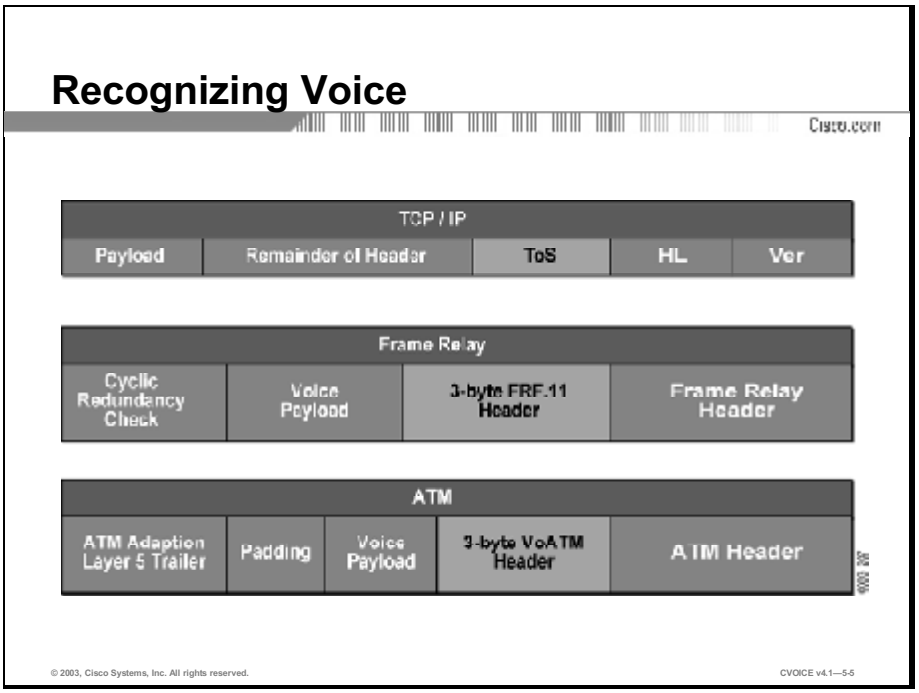


TCP/IP networks independently and individually route packets. In the figure, the router reads each packet destination address, and based on the best path at that particular moment, routes the packet toward its ultimate destination. The advantage of this approach is that areas of network failure are automatically found and packets are routed around them. The disadvantage of this approach is that packets may arrive at the destination out of sequence, resulting in arrival delays.

In Voice over ATM (VoATM) and Voice over Frame Relay (VoFR) networks, data units, such as cells in VoATM and frames in VoFR, switch through each node in the network using fixed tables. These tables enable the switches to determine the appropriate outgoing physical port for incoming data units. In the figure, the path through a VoFR or VoATM network is fixed. VoATM and VoFR switches have the ability to reroute, but the mechanism is not as fast as the dynamic routing protocol used in IP. The advantage of this approach is that the data units arrive in sequence. The disadvantage is that, on network failures, ATM and Frame Relay virtual circuits are unusable until their switch tables are rewritten.

Recognizing Voice Packets in a Stream of Voice and Data

This topic describes how voice data packets are recognized by TCP/IP, VoFR, and VoATM.



Due to problems associated with delivery of real-time traffic such as voice, a method of identifying the voice PDU is necessary. If the voice-carrying PDUs are recognized, you can apply certain quality of service (QoS) measures to expedite their transmission through the network.

Example

The table illustrates the process that TCP/IP uses to recognize voice traffic.

Table 1: Recognizing Voice Traffic in TCP/IP

Stage	What Happens
ToS (Type of Service) field in the IP header marks the packet.	The packet is marked as a priority packet.
Network devices receive the packet.	Network devices act on the priority level in the CoS field.
The priority level is recognized by the network devices.	The network devices dispatch the packet according to priority level.

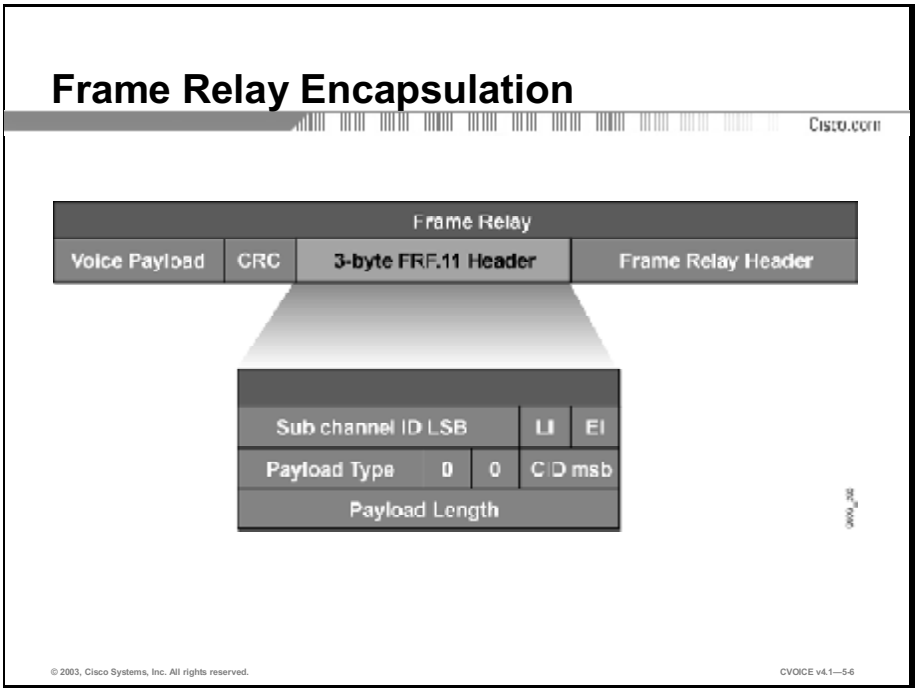
In the figure, VoFR uses a special header called Frame Relay Forum standard 11 (FRF.11). FRF.11 header is a minimum of 3 bytes in length and identifies such things as payload type and subchannels (multiple call capability). Some VoFR service providers recognize the FRF.11 header to provide preferential treatment to voice frames at a cost to the customer.

When carrying compressed voice, VoATM devices use the same 3-byte header that is used for VoFR. This 3-byte header is added to the end of the required 5-byte VoATM header to identify payload type and subchannels. If VoATM providers recognize the header, they ensure priority treatment for the voice cells.

The ATM Forum has developed various standards for transporting VoATM. These standards address many aspects of voice telephony transport over ATM, and the cells take various forms depending on the standard used.

Voice over Frame Relay Encapsulation

This topic lists the various FRF.11 fields used to encapsulate voice packets in VoFR.



Voice encapsulation with VoFR uses the format specified in FRF.11. It specifies that a minimum 3-byte header must follow the required VoFR header. Its fields are defined as follows:

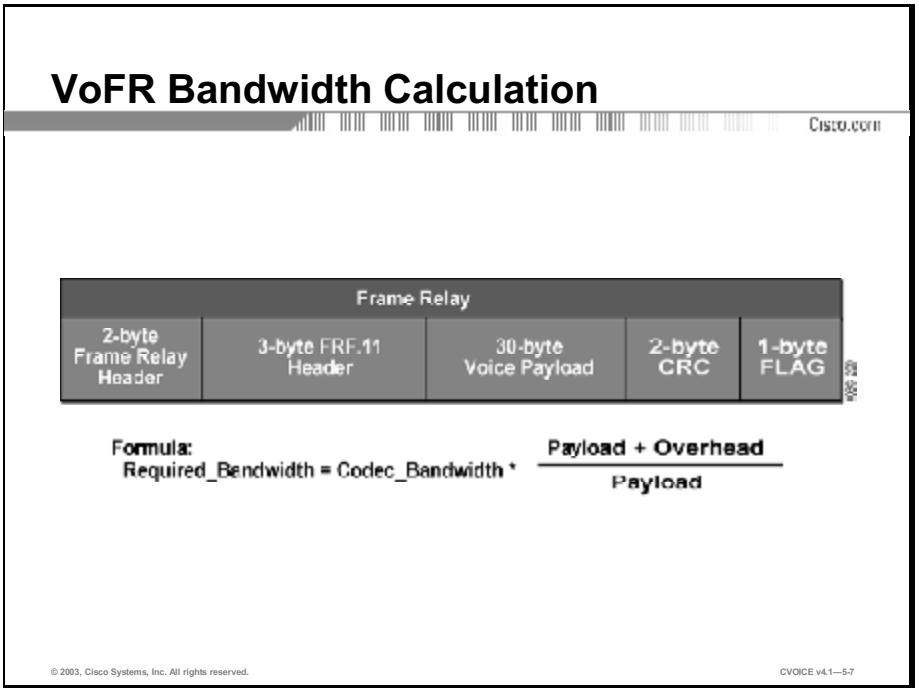
- **Subchannel ID least significant bits (LSB):** Indicates the least-significant 6 bits of the subchannel. The subchannel differentiates between separate voice calls across a common data-link connection identifier (DLCI).
- **Length Indicator (LI):** Indicates that the payload length field is present.
- **Extension Indicator (EI):** Indicates that the payload type and CID MSB fields are present.
- **Payload Type:** Indicates the contents of the payload. The contents could be fax, voice, or dialed digits.
- **0:** Indicates that the field is reserved for future use. Fields marked with “0” are always set to “0.”
- **Channel ID most significant bits (CID MSB):** Indicates the most significant bits of the subchannel ID.
- **Payload Length:** Indicates the length of the payload field. Presence of this field indicates two or more subframes contained in the payload field.

Certain versions of Cisco IOS® software make it possible to define the size of a payload. The ability to define the size of a payload is sometimes useful when the end-to-end network delay must be minimized. Each coder-decoder (codec) type has its own clearly defined default, as in the payload size for VoFR, where the default for the G.729 codec is 30 bytes.

Note	To configure the payload size for the voice frames, you must use the **codec** command from dial-peer configuration mode.

Calculating Voice over Frame Relay Bandwidth

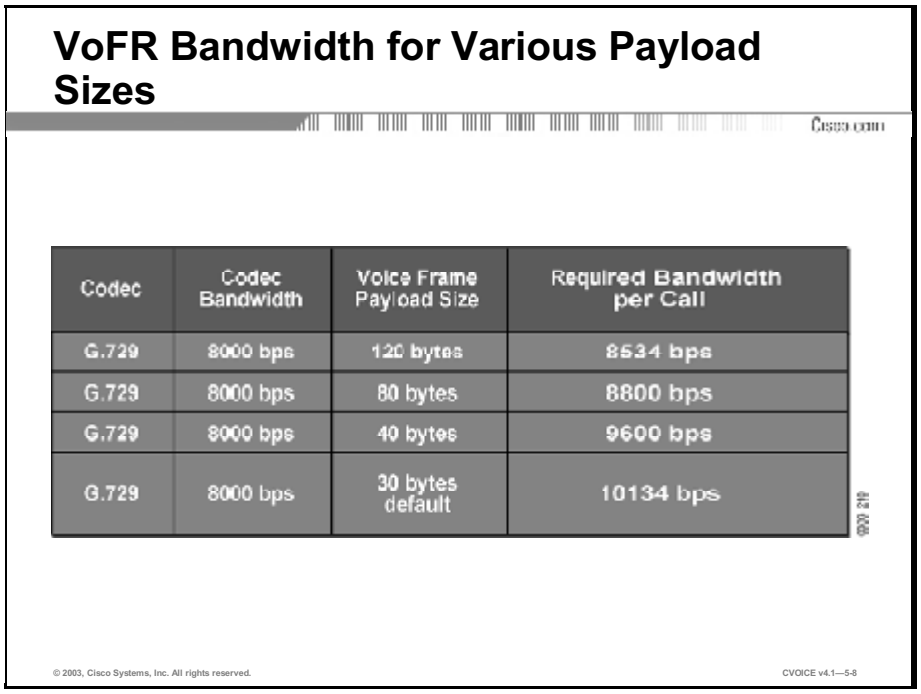
This topic describes how to calculate bandwidth requirements for various payload sizes.



Voice bandwidth used by one voice call on a VoFR network depends on these items:

- **Codec (G.729, G.711):** Different codecs require different amounts of bandwidth. For example, it takes G.711 64000 bits per second (bps) to generate one second of sound; it takes G.729 only 8000 bps to generate one second of sound.
- **Payload:** If you increase the number of bits included in each packet, the overall number of packets needed per second decreases, resulting in lower bandwidth requirements.
- **Overhead:** You can add significant overhead to the overall message with datagram information fields, such as virtual circuit identifiers (VCIs) and cyclic redundancy checks (CRCs).

You can calculate the bandwidth required for a voice call using the bandwidth of the codec, the voice packetization overhead, and the voice frame payload size. The payload size is configurable and directly affects bandwidth. The smaller the voice frame payload size, the higher the bandwidth that is required for the call.



Example

The table in the figure shows the required voice bandwidth for the G.729 8000-bps speech codec for various payload sizes using VoFR.

To make the calculation, you must use the following formula:

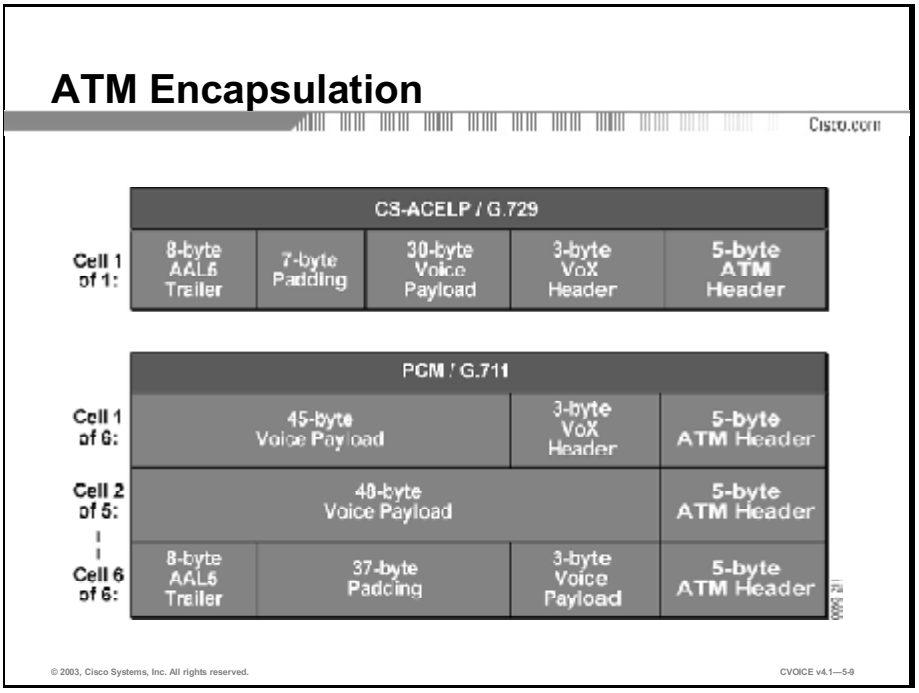
Required_Bandwidth = *Codec_Bandwidth* * [(*Overhead* + *Payload*) / *Payload*]

In this example, the default payload size for G.729, using VoFR, is 30 bytes. The bandwidth required for a G.729 call is 8000 bps. The overhead in VoFR is 2 bytes for the DLCI header, 3 bytes for the FRF.11 header, 2 bytes for the CRC, and 1 flag byte, for a total of 8 bytes. Applying the formula:

Required bandwidth = 8000 * (38 / 30) = 10134 bps

Voice over ATM Encapsulation

This topic describes the encapsulation method for VoATM.



Voice encapsulation within VoATM is limited to the cell size.

VoATM encapsulation must consider that the cell size is fixed at 53 bytes. The first 5 bytes comprise the ATM header, leaving 48 bytes left over. The VoX header uses 3 bytes, while 8 bytes are needed for the ATM Adaptation Layer (AAL5) trailer. If you use the G.729 codec, the default payload is 30 bytes, leaving a requirement for 7 bytes of padding to fill out the remainder of the cell to 53 bytes.

Note	VoX refers to nontraditional methods of carrying voice traffic. The 3-byte VoX header is exactly the same as the FRF.11 header used in Frame Relay. The 3-byte VoX header format was adopted by the ATM Forum for transport of Voice over ATM.

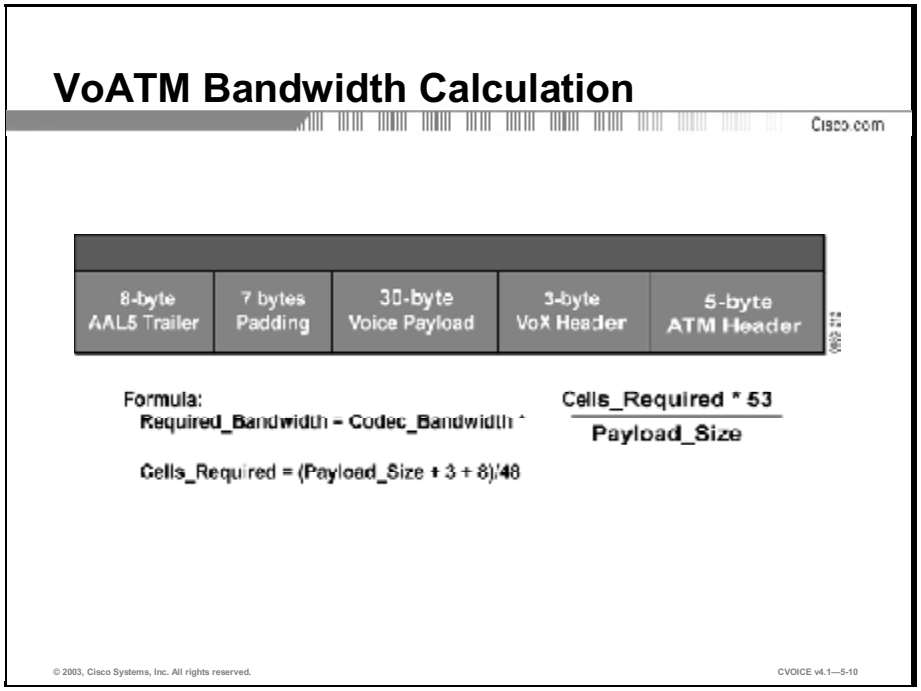
If you use a different codec, such as the G.711 codec, its default payload is 240 bytes. The default payload of 240 bytes cannot be accommodated in one single cell, so a series of six cells are used. The last cell requires 37 bytes of padding. By using other codecs and payload sizes you will vary the number of bytes that are required for padding.

It should be noted that the padding that is required in both examples is typical of VoATM and negatively affects the total required bandwidth per call.

Note	Cisco recommends AAL5 as the ATM transport mechanism for VoATM because it accommodates variable bit-rate real-time (VBR-RT) traffic.

Calculating Voice over ATM Bandwidth

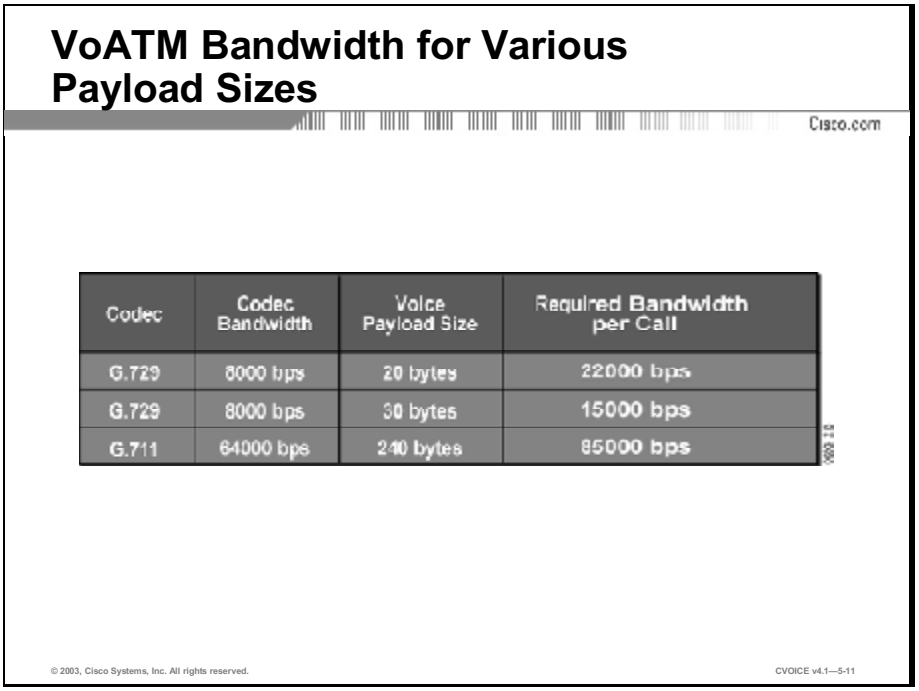
This topic describes how to determine bandwidth required for VoATM using the default and alternative encapsulation methods.



Voice bandwidth used by one voice call on a VoATM network depends on the following items:

- **Codec (G.729, G.711):** Different codecs require different amounts of bandwidth. For example, it takes G.711 64000 bps to generate one second of sound; it takes G.729 only 8000 bps to generate one second of sound.
- **Payload:** Increasing the number of bits included in each packet decreases the overall number of packets needed per second, resulting in lower bandwidth requirements.
- **Overhead:** Datagram information fields, such as VCIs and CRCs, can add significant overhead to the overall message.
- **Padding:** Because ATM uses a fixed cell size, it is necessary to "fill" unused payload bytes with padding. By varying the overall payload size and codec, you affect the amount of padding that is required.
- **Cells required:** Different codecs require a different number of cells to transmit each sample. By calculating the number of cells that are required, you take into account the voice payload, voice header, and AAL5 trailer. You must know the required number of cells to calculate the bandwidth that is required.

VoATM requires that the padding component is considered in the formula. The bandwidth required for a voice call can be calculated using the bandwidth of the codec, the voice packetization overhead, the padding that is required, and the voice payload size. The payload size is configurable and directly affects bandwidth. The smaller the voice payload size, the higher the bandwidth required for the call.



Example

The table in the figure shows the required voice bandwidth for the G.729 8000-bps speech codec for various payload sizes using VoATM.

To make the calculation, you must use the following formula and round up to a whole number:

Required_Bandwidth = *Codec_Bandwidth* * [(*Cells_Required* * 53) / *Payload_Size*]

The *Cells_Required* component is calculated and rounded up to a whole number as follows:

Cells_Required = (*Payload_Size* + 3 + 8) / 48

In the preceding calculation, the 3 and the 8 represent the VoATM header and AAL5 trailer respectively.

For example, the default payload size for G.729 using VoATM is 30 bytes. The bandwidth required for a G.729 call is 8000 bps. Apply the formula:

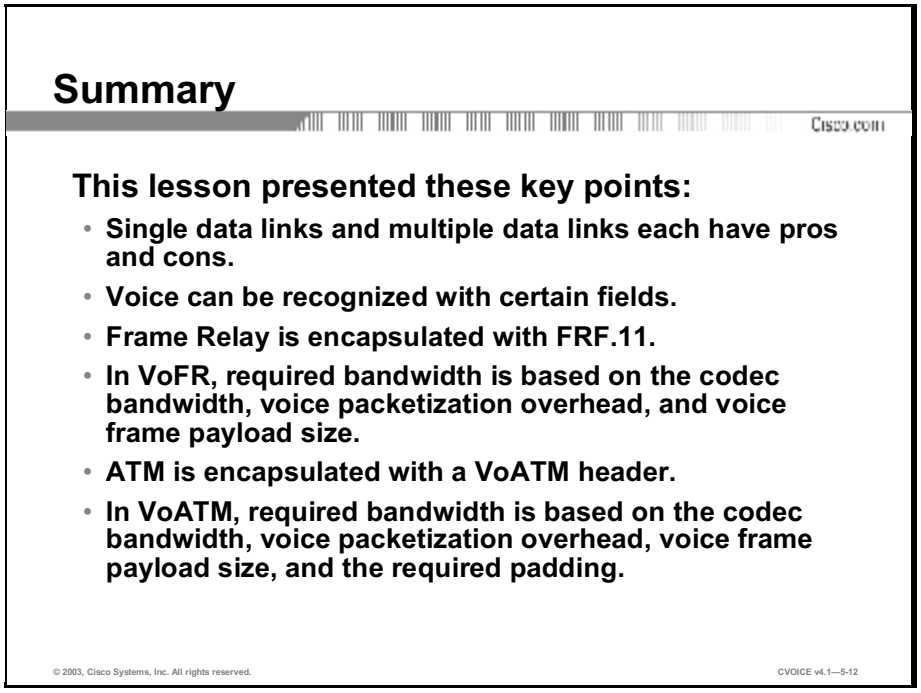
Cells_Required = (30 + 3 + 8) / 48 = 0.85, rounded to 1

Required_Bandwidth = 8000 * [(1 * 53) / 30]

Required_Bandwidth = 14.1 kbps, rounded to 15000 bps

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Voice over IP vs. Voice over Frame Relay or Voice over ATM
- Assessment (Complex Lab): Refer to Lab 5-1, contained in Laboratory Exercises in Additional Resources section E.
- Gateways and Their Roles lesson

References

For additional information, refer to these resources:

- "VoFR Encapsulation and Fragmentation" http://www.cisco.com/warp/public/788/voip/vofr_encap_frag_5733.html
- "Voice over IP (VoIP) Frame Relay (VoFR) and ATM (VoATM)" http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Technologies&f=1533

Quiz: Voice over IP vs. Voice over Frame Relay or Voice over ATM

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Compare single-path and multiple-path networks and list at least one advantage and disadvantage for each type of network
- Describe how voice packets are recognized by TCP/IP, Frame Relay, and ATM for preferential management by the technology
- Describe the functions of the Frame Relay Forum standard 11 fields that are used to encapsulate voice packets in Voice over Frame Relay
- List three variables that affect bandwidth in Voice over Frame Relay and use a formula to calculate the required bandwidth
- Describe the method of voice encapsulation that is used in Voice over ATM and provide two examples
- List five variables that affect bandwidth in Voice over ATM and use a formula to calculate the required bandwidth

Instructions

Answer these questions:

Q1) What is the advantage of VoATM and VoFR networks?

A) Data units arrive in sequence.

B) Network failures are difficult to recover from.

C) Network failures are automatically routed around.

D) Data arrives out of sequence.

Q2) What is the advantage of IP networks?

A) Data units arrive in sequence.

B) Network failures are difficult to recover from.

C) Network failures are automatically routed around.

D) Data arrives out of sequence.

Q3) Which field does TCP/IP use to mark packets as high priority?

A) FRF.11

B) payload

C) CRC

D) HL

E) ToS

Q4) In VoFR and VoATM networks, what two items does the FRF.11 header in voice packets identify? (Choose two.)

A) destination address

B) payload type

C) subchannels

D) protocol

E) version

Q5) What does the presence of the payload length field in FRF.11 encapsulation indicate?

A) the contents of the payload

B) the presence of two or more subframes in the payload field

C) the presence of the payload type and CID MSB fields

D) the most significant bits of subchannel ID

Q6) What is the default payload size for G.729 codecs using VoFR?

A) 10 bytes

B) 20 bytes

C) 30 bytes

D) 40 bytes

Q7) Which attribute of a voice packet can be configured to change the bandwidth requirements?

A) overhead

B) payload size

C) FRF.11 header

D) CRC

Q8) What would be the required bandwidth for a packet with an 80-byte payload and an 8-byte overhead if a codec with 8000 bps bandwidth is used?

A) 801 bps

B) 8000 bps

C) 8800 bps

D) 64000 bps

Q9) What is the default payload for a G.729 codec used with VoATM?

A) 30 bytes

B) 45 bytes

C) 48 bytes

D) 240 bytes

Q10) What is the size of the payload in an ATM cell?

A) 30 bytes

B) 45 bytes

C) 48 bytes

D) variable

Q11) What is the length of the AAL5 trailer in an ATM cell?

A) 3 bytes

B) 5 bytes

C) 8 bytes

D) variable

Q12) What would be the required bandwidth for a VoATM call if the payload size is 50 bytes and a G.729 codec is used?

A) 15000 bps

B) 24000 bps

C) 25000 bps

D) 85000 bps

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Gateways and Their Roles

Overview

This lesson describes the role of gateways in integrating Voice over IP (VoIP) with the traditional voice technologies that are found in enterprise and service provider networks.

Importance

Support for protocols, signaling capabilities, voice features, and voice applications is changing and growing quickly. Gateways play an important role in providing access to the right mix of functionality. You must understand the main features and functions required in enterprise and service provider environments to choose the appropriate gateway.

Objectives

Upon completing this lesson, you will be able to:

- Describe the role of gateways and their application when connecting Voice over IP to traditional public switched telephone network and telephony equipment
- Select the correct gateway to connect Voice over IP to traditional public switched telephone network and telephony equipment, given a set of guidelines
- Determine gateway interconnection requirements in an enterprise environment, given a set of guidelines
- Describe three gateway interconnection requirements in service provider environments

Learner Skills and Knowledge

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

- Understanding of telephony signaling
- Understanding the basic functions of voice gateways

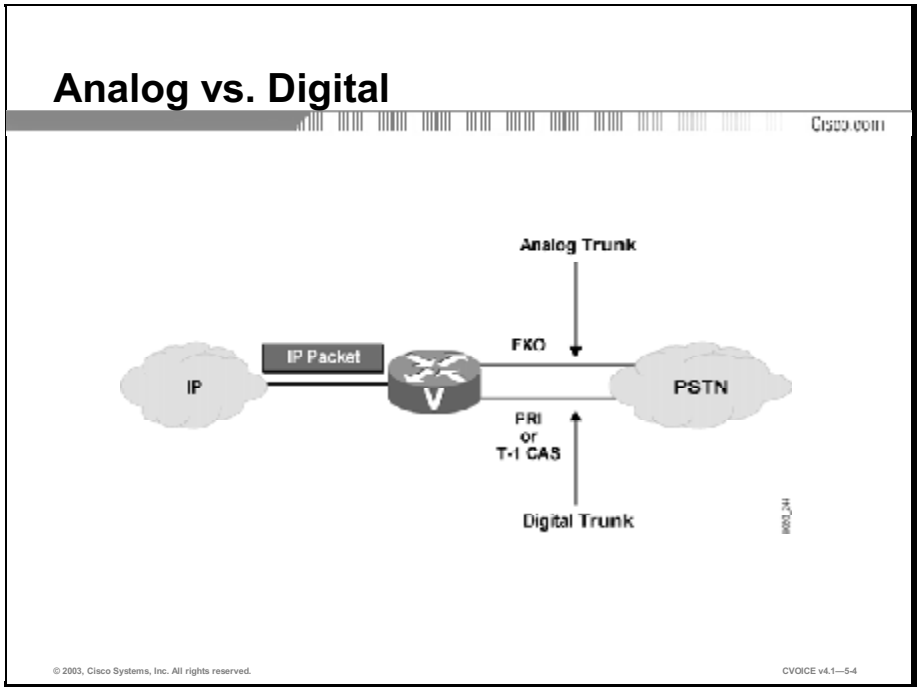
Outline

This lesson includes these topics:

- Overview
- What Are Gateways?
- Guidelines for Selecting the Correct Gateway
- Determining Gateway Interconnection Requirements in an Enterprise Environment
- Determining Gateway Interconnection Requirements in a Service Provider Environment
- Summary
- Assessment (Quiz): Gateways and Their Roles

What Are Gateways?

This topic describes the role of voice gateways and their application when connecting Voice over IP (VoIP) to traditional public switched telephone network (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; one type of gateway is the voice gateway.

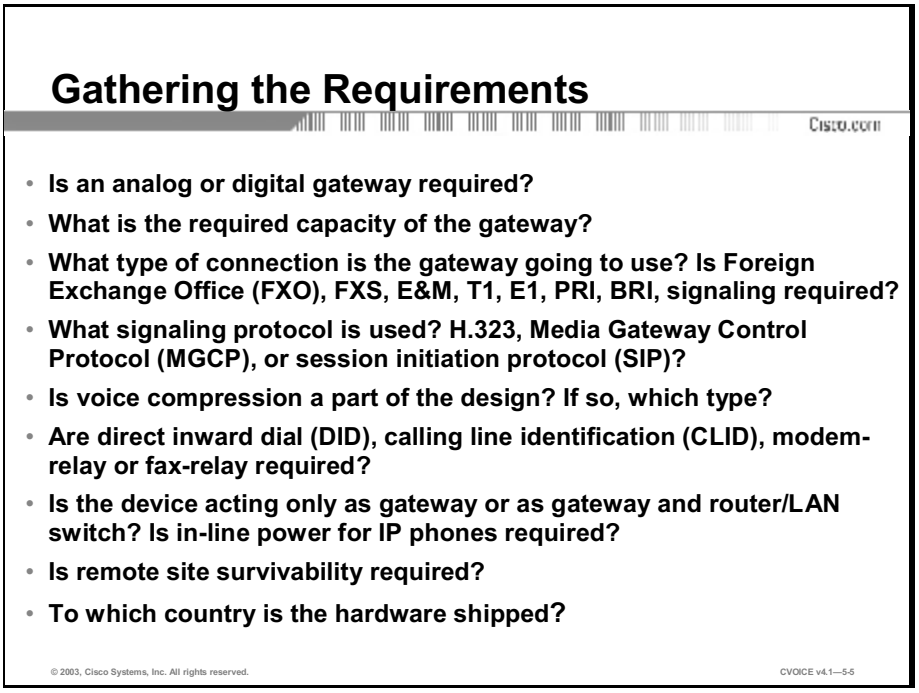
A voice gateway is a router or switch that converts IP voice packets to analog or digital signals that are understood by trunks or stations. Gateways are used in several situations, for example, connecting to the PSTN, a PBX, or a WAN link.

Example

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.

Guidelines for Selecting the Correct Gateway

This topic describes the guidelines for selecting the correct gateway.



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 be asking before installation. The answers will help to define the gateway functions and determine if the proposed design meets current requirements and encompasses future growth.

A key step is identifying the number and type of voice interfaces that are necessary and verifying the protocol support. Are supplementary services supported? Which coder-decoders (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, too, points to a specific set of hardware.

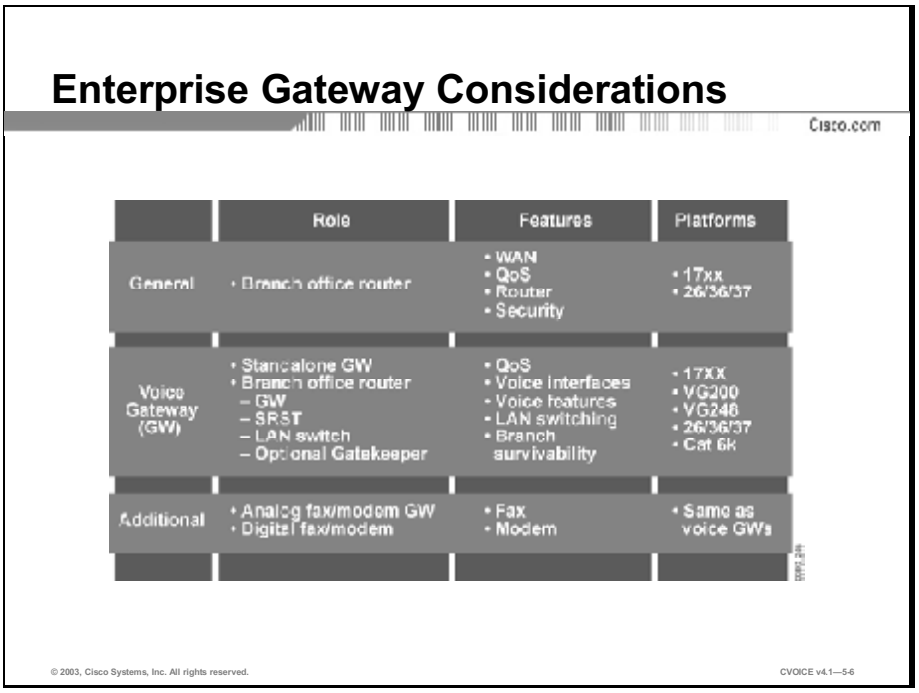
When planning gateways for location in other countries, verify that the device meets the government standards for PSTN connection in that country. Also, if the device supports encryption capabilities, verify the legality of export to the destination country.

Example

For example, if the requirements are to support Foreign Exchange Station (FXS) and recEive and transMit (E&M) connections, as well as T1 PRI from the PBX, then a suitable choice would be a Cisco 3745 Multiservice Access Router with a two-slot voice network module (VNM), 1 FXS voice interface card (VIC), 1 E&M VIC, and a high-density digital voice (HDV) module.

Determining Gateway Interconnection Requirements in an Enterprise Environment

This topic describes the guidelines for determining gateway interconnection requirements in an enterprise environment.



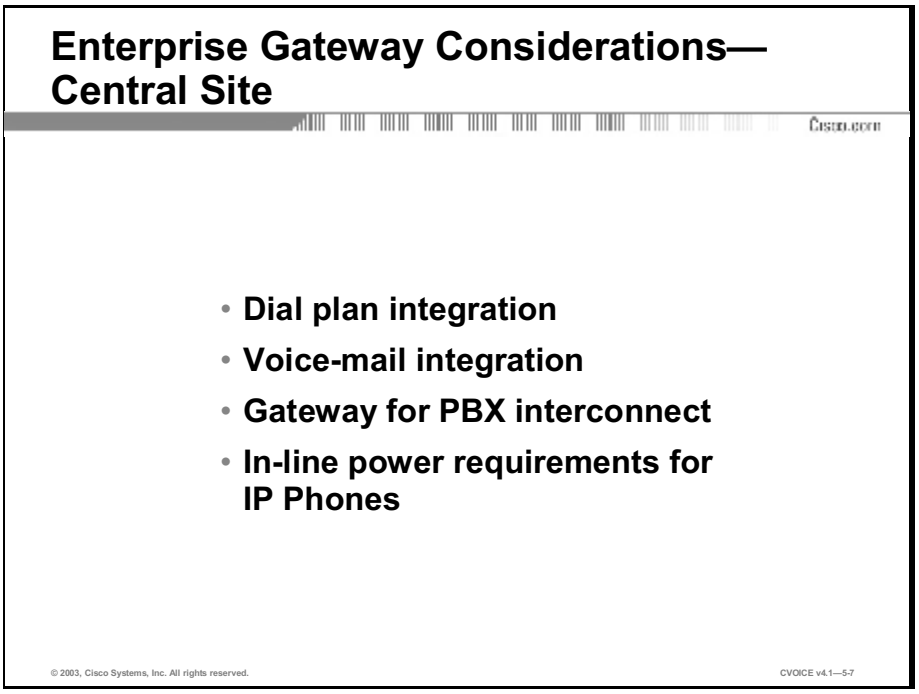
As IP telephony services become a standard in the corporate environment, a broad mix of requirements surface in the enterprise environment, IP telephony deployment typically begins by connecting to the PSTN for managing off-net calls while using a Cisco CallManager infrastructure for managing on-net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

Example

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

Table 1: Determining Gateway Interconnection Requirements

Question	Reasoning
Is the call processing distributed or centralized?	The type of call processing that is used dictates the number of gateways to deploy.
If centralized call processing is used, how do you control the gateways?	You must ensure support for proper call processing, such as MGCP.
Is cost an issue?	Distributed call processing is easier to implement, but costs are higher when deploying intelligent devices at each site.
Is remote site survivability an issue?	This 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 Survivable Remote Site Telephony (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 quality of service (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, in-line power, and security features.
Is fax or modem support required?	This requirement means the gateway must be capable of fax and modem relay functions. Another option for the enterprise customer may be 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, SIP, H.323, or MGCP.



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

- **Dial plan integration:** For consistent reachability, 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 and that all incoming calls are properly forwarded when the recipient does not answer the telephone.

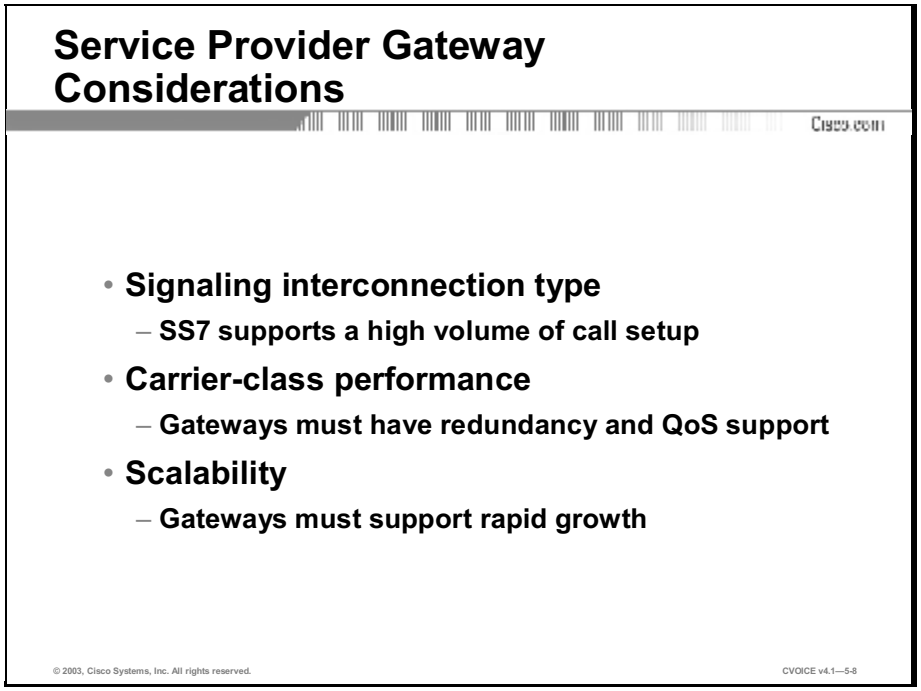
- **Gateway for PBX interconnect:** When the IP voice network interconnects PBXs, the designer must determine what type of connection is supported by the PBX and which gateway will support that connection.

- **In-line 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 in-line power to the telephones. A number of devices provide in-line power. The decision about in-line power requirements is based on capacity and the current power options.

Note	The network administrator should evaluate the need for in-line power depending on the network design.

Determining Gateway Interconnection Requirements in a Service Provider Environment

This topic provides the gateway interconnection requirements in service provider environments.



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:

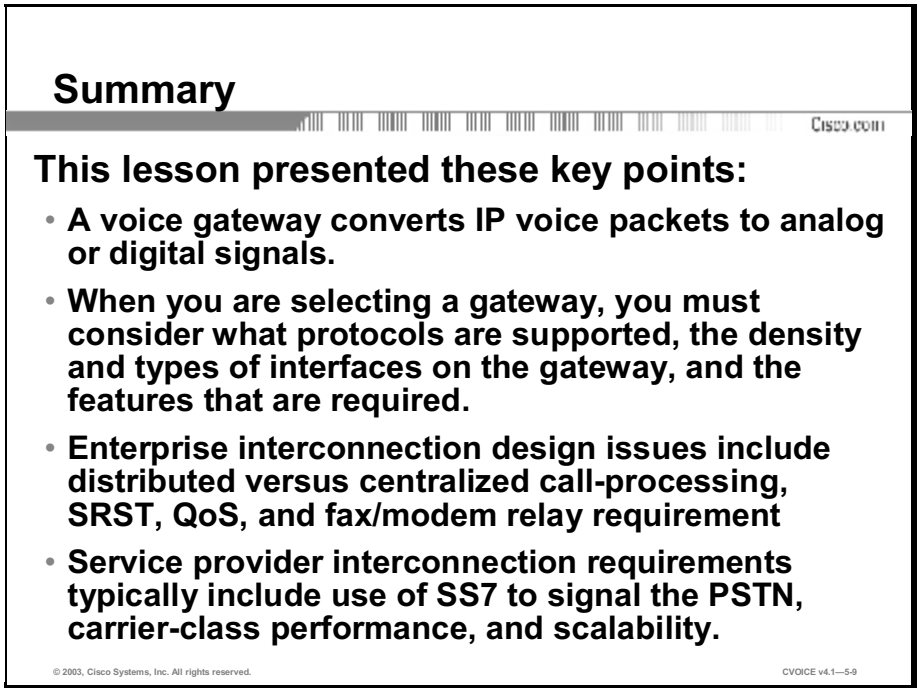
- Signaling System 7 (SS7) interconnect supports a high volume of call setup and benefits from redundant interconnect capabilities directly into the PSTN switch network.
- Carrier-class performance can be provided through the proper redundant design for high availability in addition to the proper implementation of QoS features to ensure acceptable delay and jitter.
- Scalability 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 upwards to T3 capabilities for large-scale environments.

Example

Customers looking for converged network service want service guarantees and fast service implementation. The service provider that is awarded the contract is the service provider that can deliver on customer expectations. Service providers should be prepared to sign a service level agreement (SLA) and must have the infrastructure in place to provide the required level of service. SS7 capabilities and a redundant design enable the service provider to deliver a reliable level of service.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Gateways and Their Roles
- Encapsulating Voice in IP Packets lesson

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
- "Cisco IP Communications Optimizes Enterprise Business Communications" http://www.cisco.com/en/US/netsol/ns110/ns163/ns165/ns230/networking_solutions_package.html

Quiz: Gateways and Their Roles

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the role of gateways and their application when connecting Voice over IP to traditional public switched telephone network and telephony equipment
- Select the correct gateway to connect Voice over IP to traditional public switched telephone network and telephony equipment, given a set of guidelines
- Determine gateway interconnection requirements in an enterprise environment, given a set of guidelines
- Describe three gateway interconnection requirements in service provider environments

Instructions

Answer these questions:

Q1) Which two types of devices can be used as a voice gateway? (Choose two.)

A) telephone

B) codec

C) modem

D) switch

E) router

Q2) The gateway translates the digitized signal or voice into the appropriate analog or digital signal to be sent to the PSTN based on _____.

A) the configuration of the gateway

B) the protocols being used on the network

C) the default settings of the gateway

D) the information inside the voice packet

Q3) Give two reasons why is it important to know which country the gateway will be located in when you are planning a network? (Choose two.)

A) You need to know the network requirements.

B) You need to know the standards for PSTN connections.

C) You need to know the design requirements.

D) You need to know the functions required of the gateway.

E) You need to know any legal issues involving encryption services.

Q4) Which signaling protocol can be used with gateways?

A) H.323

B) MGCP

C) SIP

D) all of the above

Q5) Issues that need to be addressed at the central site include dial plan integration, voice mail integration, gateway for PBX interconnect, and _____.

A) signaling interconnection type

B) carrier-class performance

C) scalability

D) in-line power requirements for IP phones

Q6) 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, in-line power, and security features are to be implemented.

C) It affects zone configurations.

D) It determines the Cisco IOS version that should be used.

Q7) Which feature of the service provider network benefits from redundant interconnect capabilities directly into the PSTN?

A) SS7 interconnections

B) carrier-class performance

C) scalability

D) all of the above

Q8) If implemented properly, which feature of a service provider gateway can provide carrier-class performance?

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

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Encapsulating Voice in IP Packets

Overview

This lesson discusses the Voice over IP (VoIP) protocol stack, its applied headers, and the use of Compressed Real-Time Transport Protocol (CRTP) to reduce header size.

Importance

A number of protocols and tools are used to successfully carry 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 packaging voice 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:

- Define the major VoIP protocols and how they map to the seven layers of the Open System Interconnection model
- Describe the functions of Real-Time Transport Protocol and Real-Time Transport Control Protocol as they relate to a VoIP network
- Describe how IP voice headers are compressed using CRTP
- Identify three conditions that necessitate the compression of the Real-Time Transport Protocol header

Learner Skills and Knowledge

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

- General knowledge of the seven-layer Open System Interconnection (OSI) model
- General knowledge of header compression

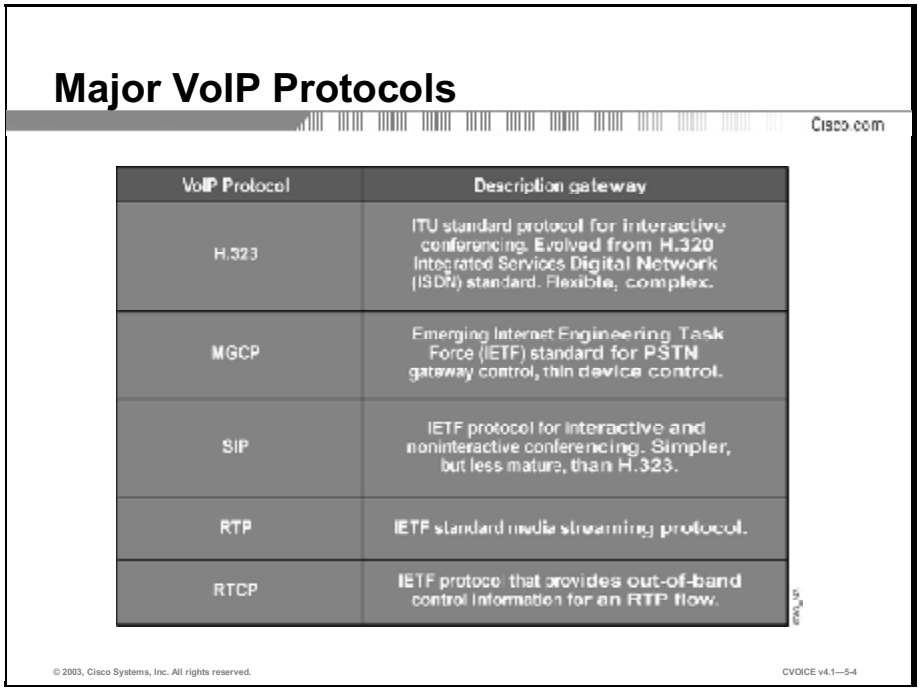
Outline

This lesson includes these topics:

- Overview
- Major VoIP Protocols
- RTP and RTCP
- Reducing Header Overhead with CRTP
- When to Use RTP Header Compression
- Summary
- Assessment (Quiz): Encapsulating Voice in IP Packets

Major VoIP Protocols

This topic defines the major Voice over IP (VoIP) protocols and matches them with the seven layers of the Open System Interconnection (OSI) model.



The major VoIP protocols include the following:

- **H.323:** An International Telecommunications Union (ITU) standard protocol for interactive conferencing. The ITU standard protocol was originally designed for multimedia in a connectionless environment, such as a LAN. The 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.

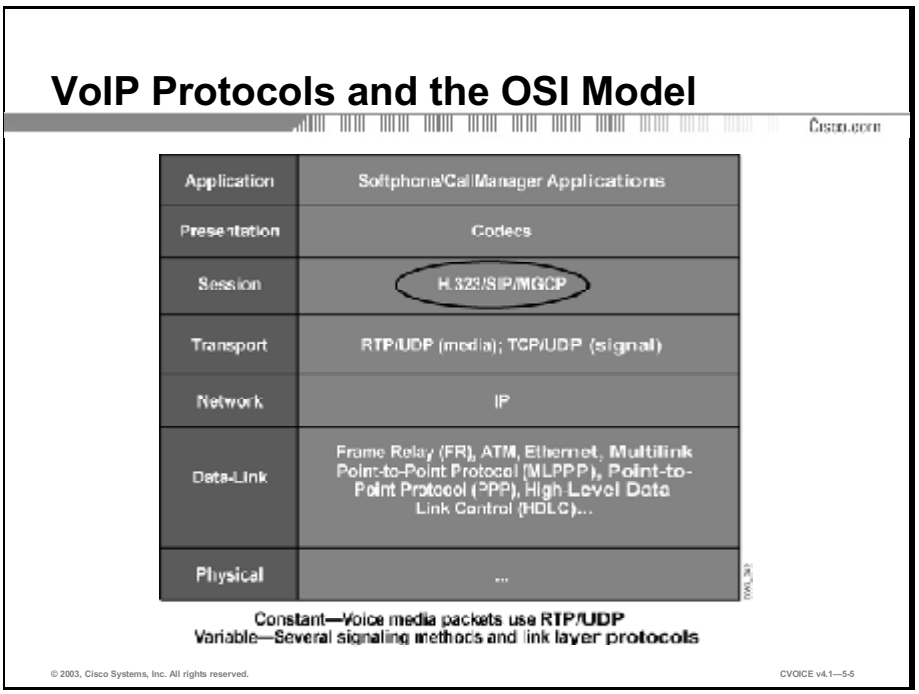
- **Media Gateway Control Protocol (MGCP):** An emerging standard for public switched telephone network (PSTN) gateway control or thin device control. Specified in RFC 2705, MGCP defines a protocol to control VoIP gateways connected to external call-control devices. MGCP provides the signaling capability for less expensive edge devices, such as gateways, that may not contain a full voice-signaling stack, such as H.323. In essence, any time an event such as off hook occurs at the voice port of a gateway, the voice port reports that event to the MGCP controller. The MGCP controller then signals that device to provide a service, such as dial-tone signaling.

- **Session Initiation Protocol (SIP):** A detailed protocol that specifies the commands and responses to set up and tear down calls. It 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 Hypertext Transfer Protocol (HTTP), using the same transaction request and/or response model and similar headers 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):** An Internet Engineering Task Force (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.

- **RTP Control Protocol (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.



Example

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

Applications such as Softphone and Cisco CallManager provide the interface for users to originate voice at their PCs or laptops and convert and compress it before passing it to the network.

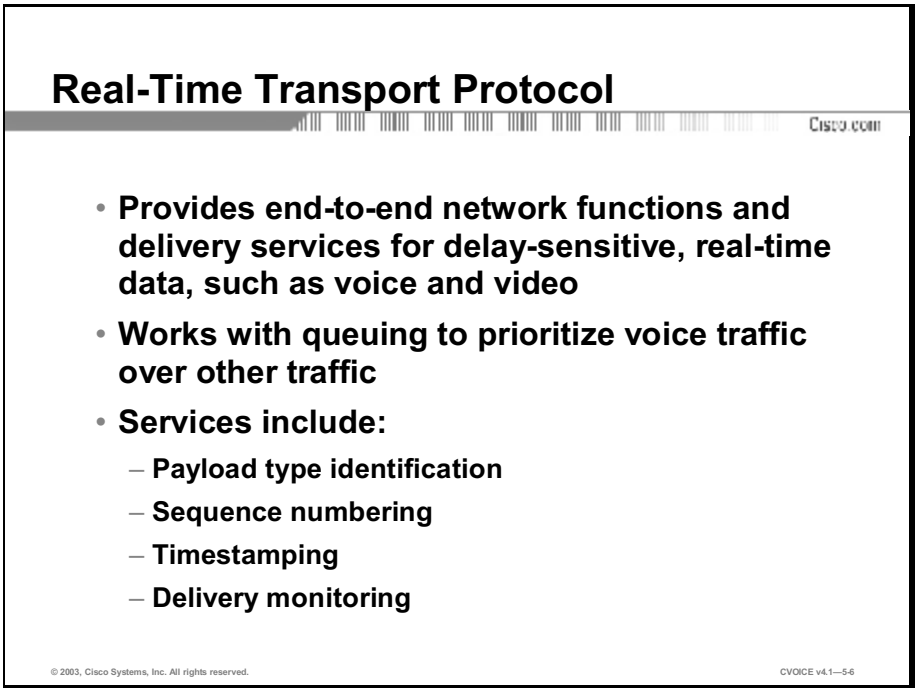
Coder-decoders (codecs) define how the voice is compressed. The user can configure which codec to use or a codec is negotiated according to what is available.

One of the constants in VoIP implementation is that voice uses RTP inside of UDP to carry the payload across the network. Because 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. Since UDP does not provide services, such as sequence numbers or time stamps, RTP provides sequencing functionality.

The variables in VoIP are the signaling methods used. H.323 and SIP define end-to-end call signaling methods. MGCP defines a method to separate the signaling function from the voice call function. MGCP uses a central control device 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.

RTP and RTCP

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



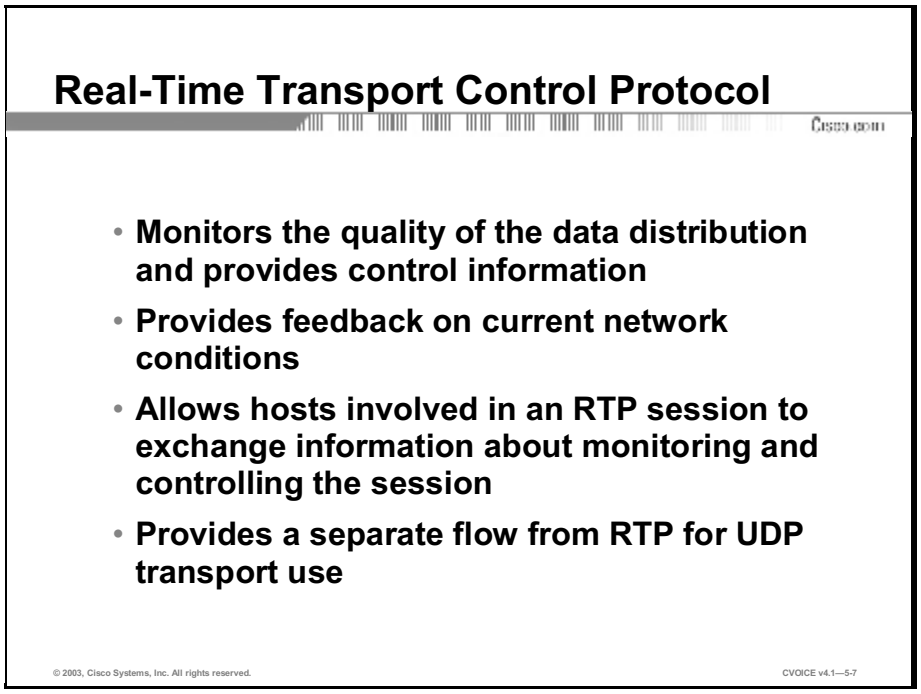
RTP provides end-to-end network transport functions intended for applications transmitting real-time requirements, such as audio and video. Those functions include payload type identification, sequence numbering, time stamping, and delivery monitoring.

RTP typically runs on top of UDP to utilize 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.

Example

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 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.

For more information on RTP, refer to RFC 1889.



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

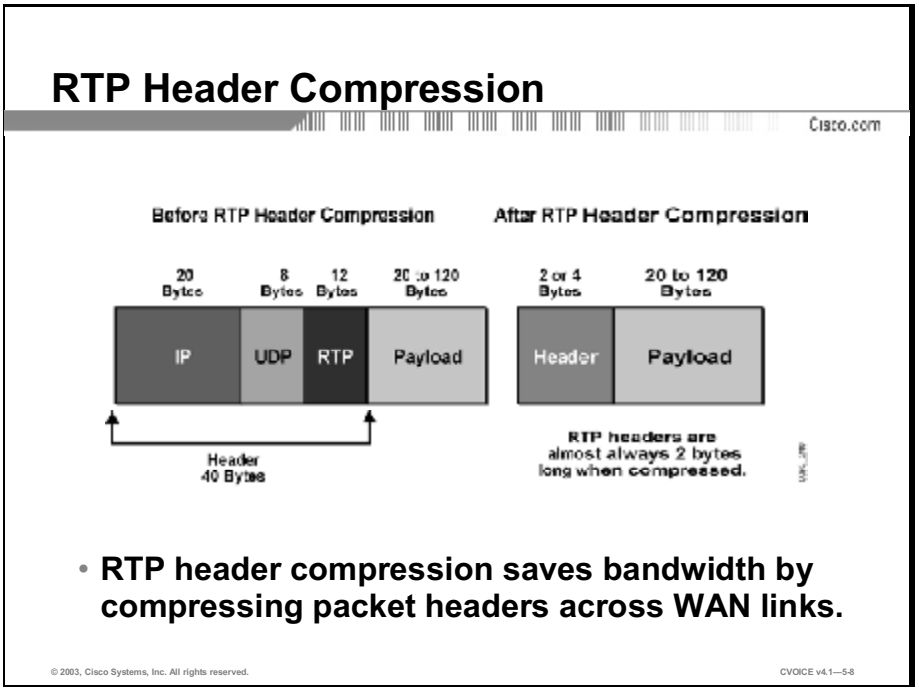
- RTCP provides a separate flow from RTP for transport use by UDP. When a voice stream is assigned UDP port numbers, RTP is typically assigned an even-numbered port and RTCP is assigned the next odd-numbered port. Each voice call has four ports assigned: RTP plus RTCP in the transmit directions and RTP plus RTCP in the receive direction.

Example

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 that includes packet count, octet count, number of packets lost, and jitter. The RTCP header information would shed light on why the calls were disconnected.

Reducing Header Overhead with CRTP

This topic describes how IP voice headers are compressed using Compressed Real-Time Transport Protocol (CRTP).



Given the number of multiple protocols that are necessary to transport voice over an IP network, the packet header can be large. You can use cRTP headers on a link-by-link basis to save bandwidth.

Using CRTP compresses the IP/UDP/RTP header from 40 bytes to 2 bytes without UDP checksums and from 40 bytes to 4 bytes with UDP checksums. RTP header compression is especially beneficial when the RTP payload size is small; for example, with compressed audio payloads between 20 and 50 bytes.

In addition, CRTP works on the premise that most of the fields in the IP/UDP/RTP header do not change, or that the change is predictable. Static fields include source and destination IP address, source and destination UDP port numbers, as well as many other fields in all three headers. For those fields where the change is predictable, the CRTP process is illustrated in the following table:

Table 1: CRTP

Stage	What Happens
The change is predictable.	The sending side tracks the predicted change.
The predicted change is tracked.	The sending side sends a hash of the header.
The receiving side predicts what the constant change is.	The receiving side substitutes the original stored header and calculates the changed fields.
There is an unexpected change.	The sending side sends the entire header without compression.

CRTP Packet Components

In a packet voice environment when speech samples are framed every 20 ms, a payload of 20 bytes is generated. Without CRTP, the total packet size includes the following components:

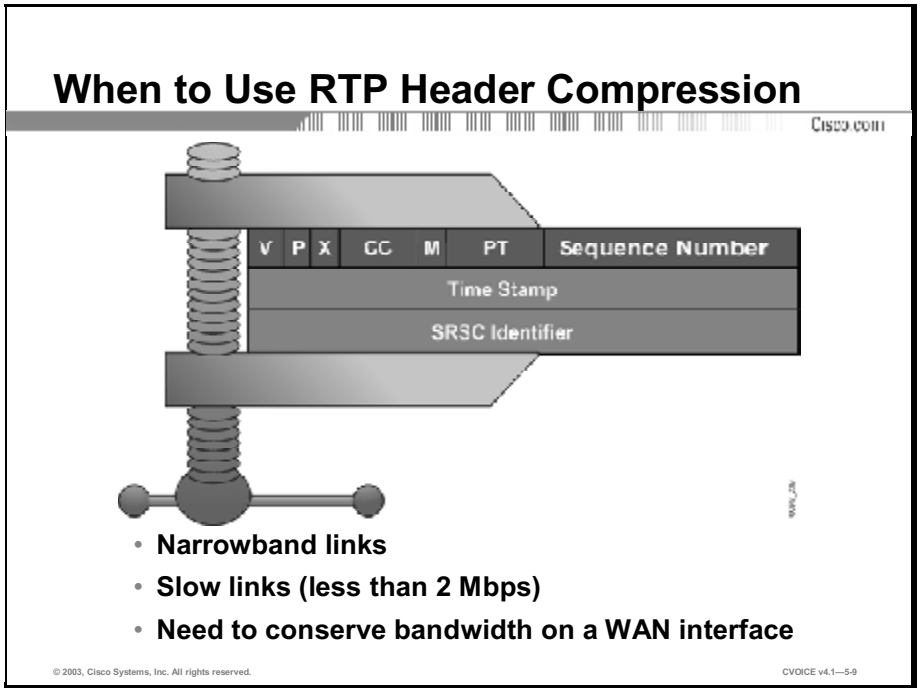
- IP header (20 bytes)
- UDP header (8 bytes)
- RTP header (12 bytes)
- Payload (20 bytes)

The header is twice the size of the payload; IP/UDP/RTP (20 + 8 + 12 = 40 bytes) vs. payload (20 bytes). When generating packets every 20 ms on a slow link, the header consumes a large portion of bandwidth.

In the figure, RTP header compression reduces the header to 2 bytes. The compressed header is $1/10^{th}$ the payload size.

When to Use RTP Header Compression

This topic describes when to use CRTP.



You must configure CRTP on a specific serial interface or subinterface if you have any of these conditions:

- Narrowband links
- Slow links (less than 2 Mbps)
- Need to conserve bandwidth on a WAN interface

Compression works on a link-by-link basis and must be enabled for each link that fits these requirements. You must enable compression on both sides of the link for proper results. Enabling compression on both ends of a low-bandwidth serial link can greatly reduce the network overhead if there is a significant volume of RTP traffic on that slow link.

Note	Compression adds to processing overhead. You must check resource availability on each device prior to turning on RTP header compression.

Example

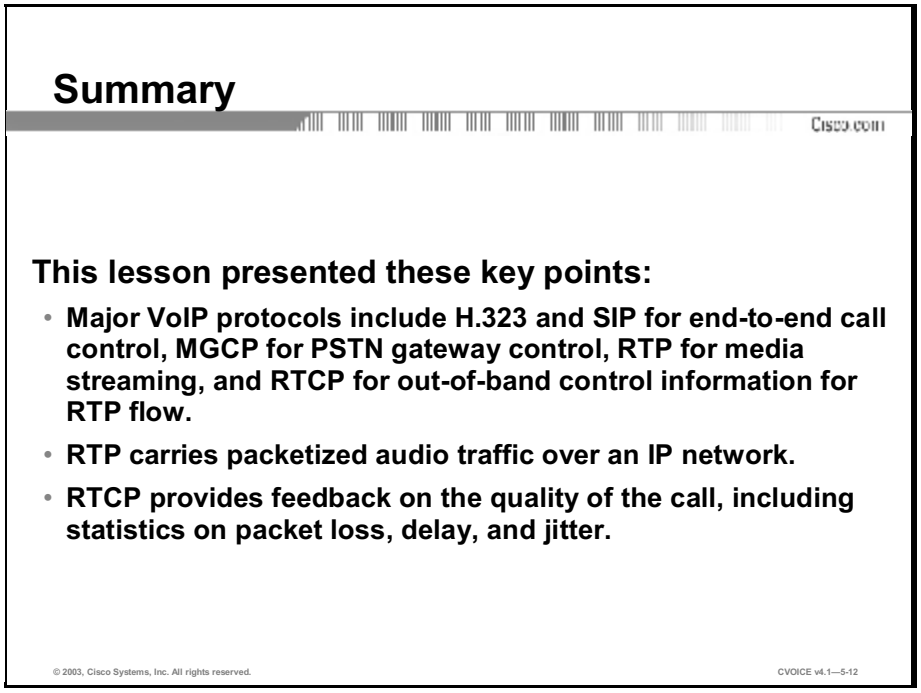
If you want the router to compress RTP packets, use the **ip rtp header-compression** command. The **ip rtp header-compression** command defaults to active mode when it is configured. However, this command provides a passive mode setting in instances where you want the router to compress RTP packets *only* if it has received compressed RTP on that interface. When applying to a Frame Relay interface, use the **frame-relay ip rtp header-compression** command.

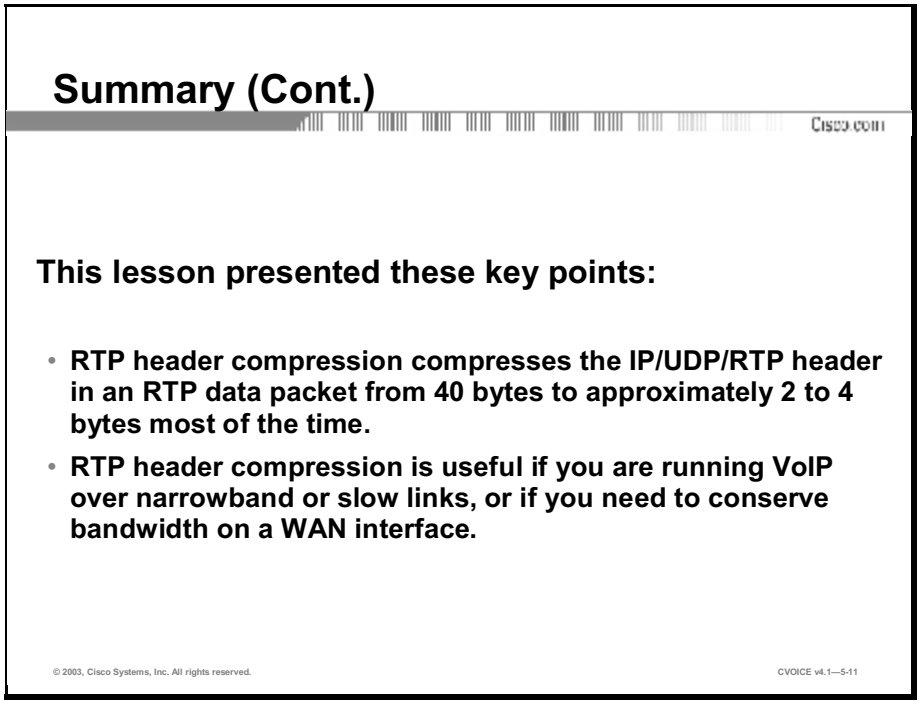
By default, the software supports a total of 16 RTP header compression connections on an interface. Depending on the traffic on the interface, you can change the number of header compression connections with the **ip rtp compression-connections** *number* command.

Note	Do not use CRTP if you have high-speed interfaces or links faster than 2 Mbps.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Encapsulating Voice in IP Packets
- Bandwidth Requirements lesson

References

For additional information, refer to these resources:

- "Request for Comments"
  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

Quiz: Encapsulating Voice in IP Packets

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Define the major VoIP protocols and how they map to the seven layers of the Open System Interconnection model
- Describe the functions of Real-Time Transport Protocol and Real-Time Transport Control Protocol as they relate to a VoIP network
- Describe how IP voice headers are compressed using CRTP
- Identify three conditions that necessitate the compression of the Real-Time Transport Protocol header

Instructions

Answer these questions:

Q1) Match the VoIP protocol with its function.

A) H.323

B) MGCP

C) SIP

D) RTP

E) RTCP

_____ 1. adopts a modified form of the URL addressing scheme used within e-mail based on SMTP

_____ 2. allows control of VoIP gateways connected to external call control devices

_____ 3. reports statistics on the call

_____ 4. defines all aspects of synchronized voice, video, and data transmission

_____ 5. provides sequence numbers and time stamps for orderly processing of voice packets

Q2) Which VoIP protocol operates at the transport layer of the OSI model?

A) H.323

B) MGCP

C) SIP

D) RTP

Q3) An RTP is primarily designed for which type of session?

A) unicast

B) multicast

C) broadcast

D) all of the above

Q4) Which Layer-4 protocol is used for transporting RTCP packets?

A) IP

B) TCP

C) UDP

D) RTP

Q5) What is the size of the IP/UDP/RTP header?

A) 20 bytes

B) 32 bytes

C) 40 bytes

D) 48 bytes

Q6) To what size does CRTP compress the IP/UDP/RTP header when UDP checksums are used?

A) 2 bytes

B) 4 bytes

C) 8 bytes

D) 12 bytes

Q7) Which two conditions necessitate the use of CRTP? (Choose two.)

A) need for bandwidth conservation on WAN interfaces

B) high-speed interfaces

C) links that are as slow as 4 Mbps

D) narrowband links

E) broadband links

Q8) Where should compression be enabled?

A) on each link that requires it

B) on the entire network

C) on both sides of a slow link

D) on links with high traffic

E) on all links using RTP

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

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.

Importance

Since 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 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
- 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 voice activity detection

Learner Skills and Knowledge

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

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

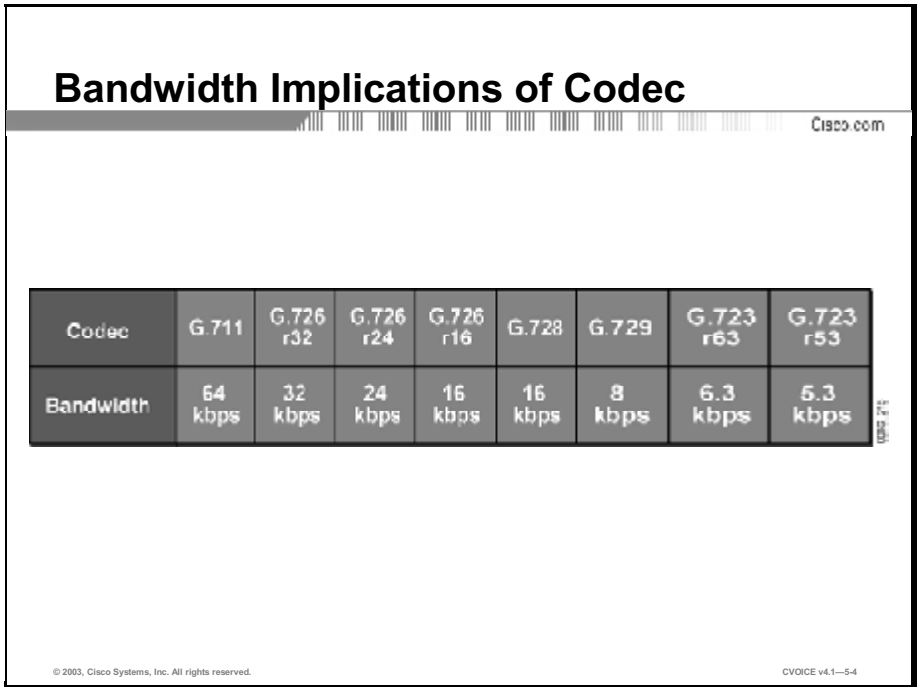
Outline

This lesson includes these topics:

- Overview
- Codec Bandwidths
- Impact of Voice Samples and Packet Size on Bandwidth
- Data Link Overhead
- Calculating the Total Bandwidth for a VoIP Call
- Effects of Voice Activity Detection on Bandwidth
- Summary
- Assessment (Quiz): Bandwidth Requirements

Codec Bandwidths

This topic describes the bandwidth that each coder-decoder (codec) uses and illustrates its impact on total bandwidth.



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 Voice over IP (VoIP) call. With a thorough understanding of VoIP bandwidth, the network administrator can apply capacity-planning tools.

Following is a list of codecs and their associated bandwidth.

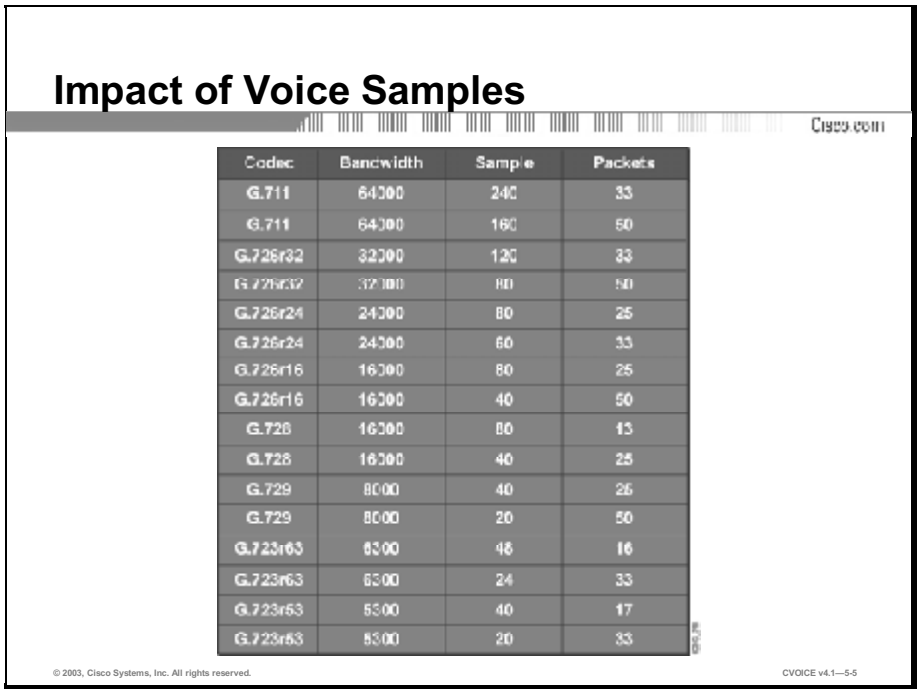
- The G.711 pulse code modulation (PCM) coding scheme uses the most bandwidth. It takes samples 8000 times per second, each of which is 8 bits in length, for a total of 64000 bps.
- The G.726 adaptive differential pulse code modulation (ADPCM) coding schemes use somewhat less bandwidth. While each coding scheme takes samples 8000 times per second like PCM, it uses 4, 3, or 2 bits for each sample. The 4, 3, or 2 bits for each sample results in total bandwidths of 32000, 24000, or 16000 bps.
- The G.728 low delay-code excited linear prediction (LD-CELP) coding scheme compresses PCM samples using codebook technology. It uses a total bandwidth of 16000 bps.
- The G.729 and G.729a Conjugate Structure Algebraic Code Excited Linear Prediction (CS-ACELP) coding scheme also compresses PCM using advanced codebook technology. It uses 8000 bps total bandwidth.

- The G.723 and G.723a multipulse maximum likelihood quantization (MPMLQ) coding schemes use a look-ahead algorithm. These compression schemes result in 6300 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, the higher the cost of each call across the network.

Impact of Voice Samples and Packet Size on Bandwidth

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



Voice sample size is a variable that can affect 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 output samples 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

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):

Bytes_per_Sample = (*Sample_Size* * *Codec_Bandwidth*) / 8

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

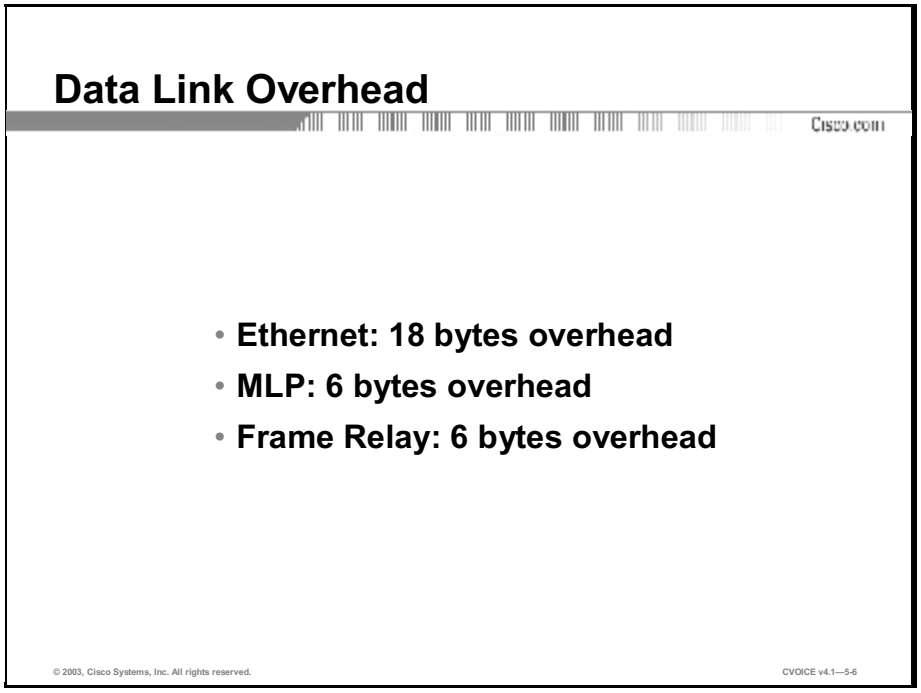
Bytes_per_Sample = (.020 x 64000) / 8

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.

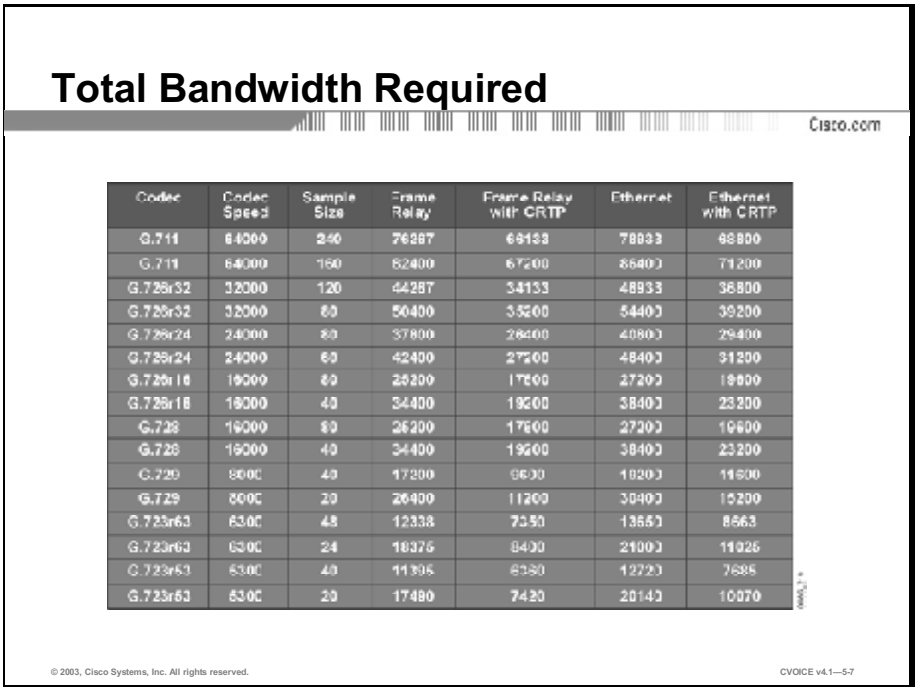


Another contributing factor to bandwidth is the Layer 2 protocol used to transport VoIP. VoIP alone carries a 40-byte IP/User Datagram Protocol/Real-Time Transport Protocol (IP/UDP/RTP) header, assuming uncompressed RTP. Depending on the Layer 2 protocol used, the overhead could grow substantially. The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

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.



Codec choice, data-link overhead, sample size, and even compressed RTP, all have positive and negative impacts on total bandwidth. To perform the calculations, you must have all of the 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

The following calculation was used to produce the figure:

Total_Bandwidth = ([*Layer_2_Overhead* + *IP_UDP_RTP Overhead* + *Sample_Size*] / *Sample_Size*) * *Codec_Speed*

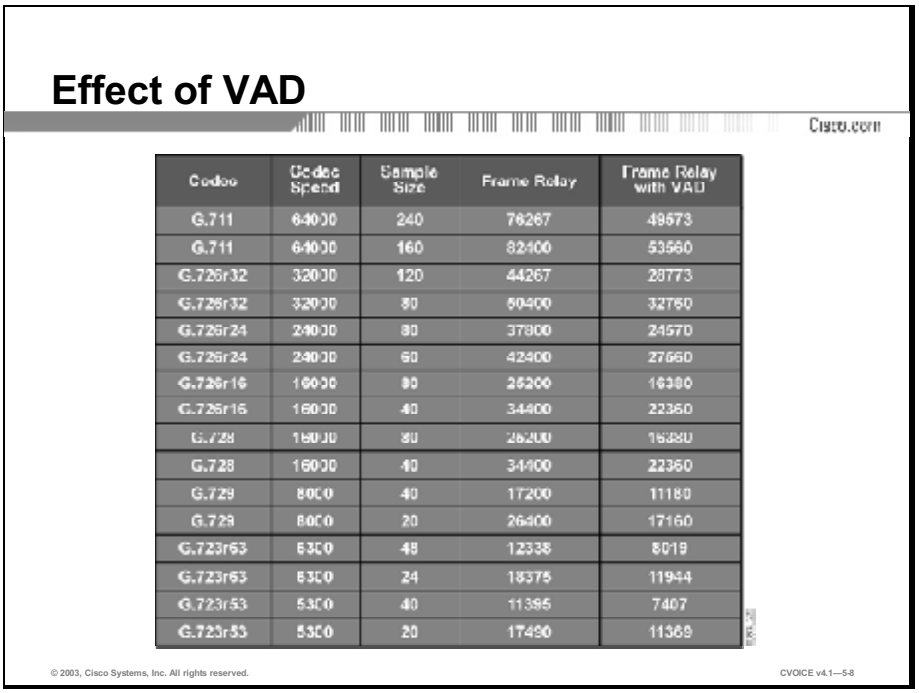
For example, assume a G.729 codec, 20-byte sample size, using Frame Relay without compressed Real-Time Transport Protocol (cRTP):

Total_Bandwidth = ([6 + 40 +20]/20) * 8000

Total_Bandwidth = 26400 bps

Effects of Voice Activity Detection on Bandwidth

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



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. With Cisco VoIP networks, all conversation and silence is 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.

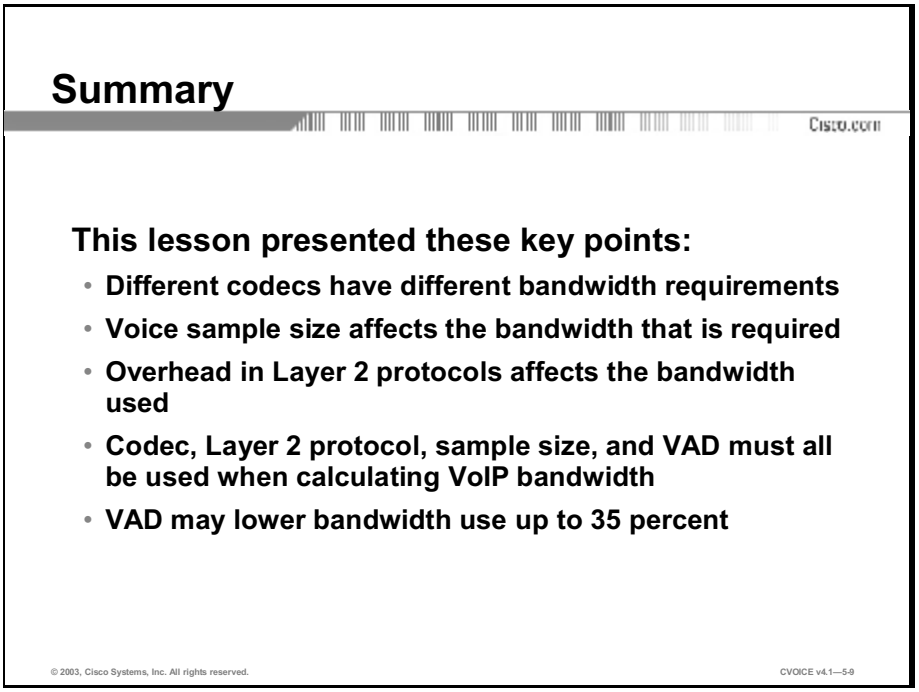
VAD is enabled by default for all VoIP calls. VAD reduces the silence in VoIP conversations but it also provides comfort noise generation (CNG). Because you can mistake silence for a disconnected call, CNG provides locally generated *white noise* to make the call appear normally connected to both parties.

Example

The figure shows examples of the VAD effect in a Frame Relay VoIP environment. In the example using G.711 with a 160-byte payload, the bandwidth required is 82400 bps. By turning VAD on, you can reduce the bandwidth utilization to 53560bps. This is a savings of 35 percent bandwidth.

Summary

This topic summarizes the key point discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Bandwidth Requirements
- Security Implications lesson

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#related
- "Voice over IP (VoIP) Frame Relay (VoFR) and ATM (VoATM)"
  http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Technologies&f=1533

Quiz: Bandwidth Requirements

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- 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
- 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 voice activity detection

Instructions

Answer these questions:

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 it uses.

A) G.711

B) G.726

C) G.728

D) G.729

E) G.723

_____ 1. ADPCM

_____ 2. CS-ACELP

_____ 3. LD-CELP

_____ 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 would be the size of voice samples from Cisco voice equipment if a G.728 codec were used?

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) Which factor lowers bandwidth requirements for a VoIP call?

A) larger sample size

B) more bandwidth required by the codec

C) more overhead associated with the data link

D) none of the above

Q8) 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) 11600 bps

C) 17200 bps

D) 19200 bps

Q9) What is the function of comfort noise generation?

A) provides features such as MOH

B) provides white noise to make the call appear normally connected to both parties

C) provides full voice call bandwidth

D) reduces the delay in VoIP connections

Q10) If the bandwidth requirement for a voice call over Frame Relay is 11395 bps, what would be the bandwidth requirement if VAD was used?

A) 3989 bps

B) 7407 bps

C) 9116 bps

D) 11180 bps

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Security Implications

Overview

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

Importance

Security is a top priority in most networks. The many types of 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 in-depth knowledge of existing security measures and how they affect the transit of voice through the network.

Objectives

Upon completing this lesson, you will be able to:

- Describe three elements of a security policy that are necessary for a Voice over IP network
- Describe the dynamic access control process used by firewalls to allow voice packets to pass
- Outline the steps needed to reduce overhead and delay for Voice over IP in a VPN
- Describe how to calculate the bandwidth required for a VPN packet

Learner Skills and Knowledge

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

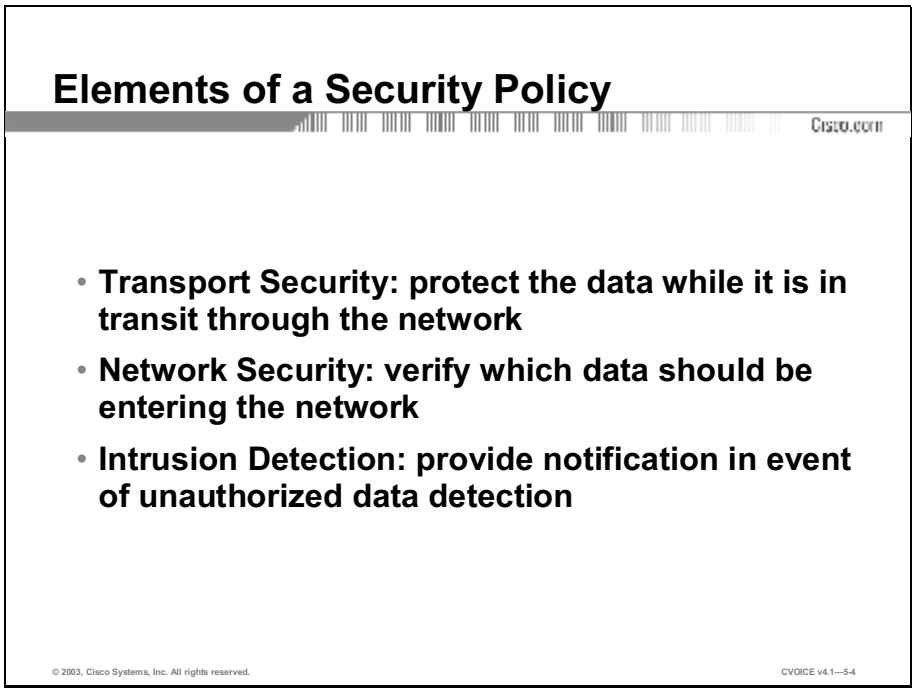
- General knowledge of VPNs
- General knowledge of firewalls
- Understanding of voice requirements, including delay and port numbering

Outline

This lesson includes these topics:

- Overview
- Security Policies for Voice over IP Networks
- Communicating Through a Firewall
- Delivery of Voice over IP Through a VPN
- Bandwidth Overhead Associated with VPN
- Summary
- Assessment (Quiz): Security Implications

Security Policies for Voice over IP Networks



This topic describes the elements of a security policy for a Voice over IP (VoIP) network. 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. The requirements for secured IP telephony include the following:

- It must provide ubiquitous IP telephony services to the locations and to the users that require it.
- It must maintain as many of the characteristics of traditional telephony as possible, while doing so in a secure manner.
- It must integrate with existing security architecture and not interfere with existing functions.

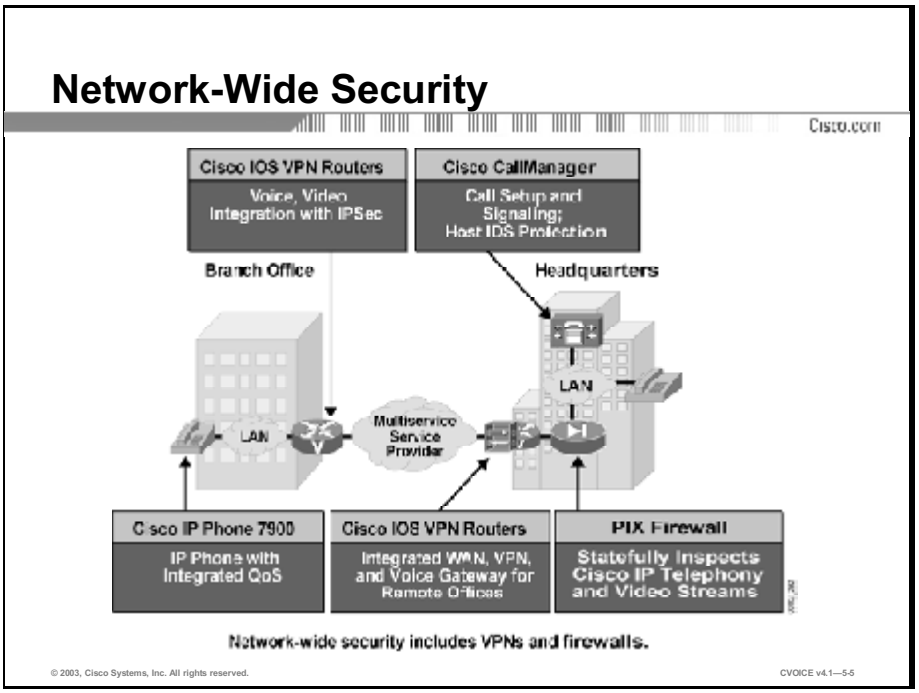
The starting point for any security implementation is the development of a security policy. In a converged network, the security policy must account for the impact of security measures on voice traffic. The security policy should address the following points that affect voice:

- **Transport security:** Traffic traversing public access and backbone networks must be properly secured. IP Security (IPSec) and Virtual Private Networks (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 it in 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, then the traffic passing through the firewall is encrypted and is subject to stateful inspection. If the VPN terminates outside the firewall, then the firewall has access to Real-Time Transport Protocol/User Datagram Protocol/TCP/IP (RTP/UDP/TCP/IP) headers and is able to inspect the packet for call setup.

- **Intrusion detection:** In the event of an attempted attack, intrusion detection plays an integral part in securing a network by providing additional network perimeter protection and proactive notification.

Example

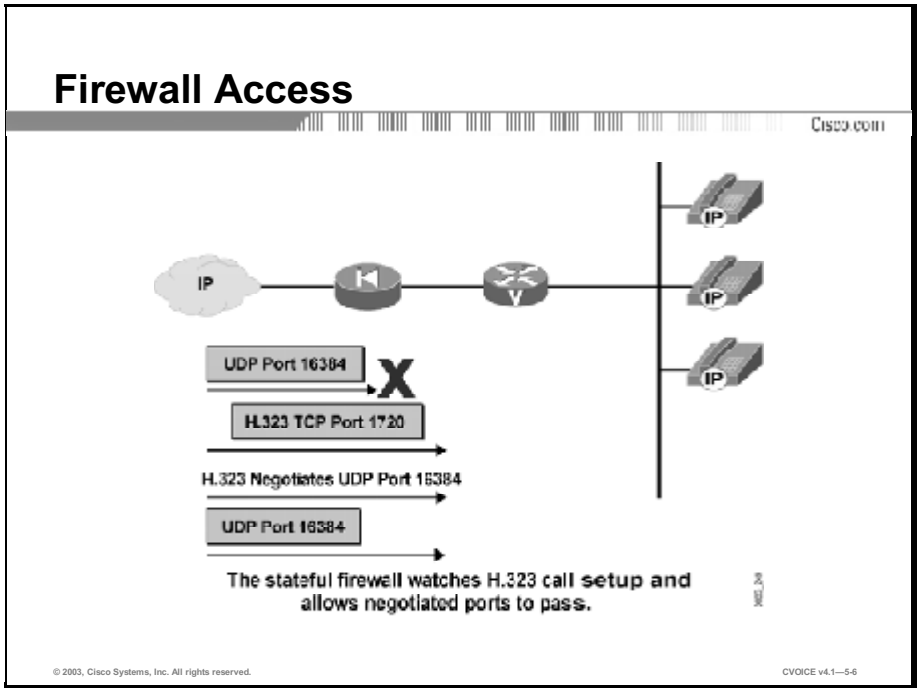


In the figure, the network between the branch office and the headquarters has a firewall. The firewall allows the users from the branch office only to access the headquarters network. A user without proper network identification will not be allowed to pass through the firewall. Network identification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

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

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 process is called *stateful inspection of packets*. In addition to checking static ports and recognizing protocols that negotiate dynamic ports (for example, H.323), the firewall looks into the packets of that protocol to track the flows.

Example

In the figure, any application may use a port in the range of 1024 to 65536. 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.

Table 1: 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 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 the firewall has the proper resources to handle the load.

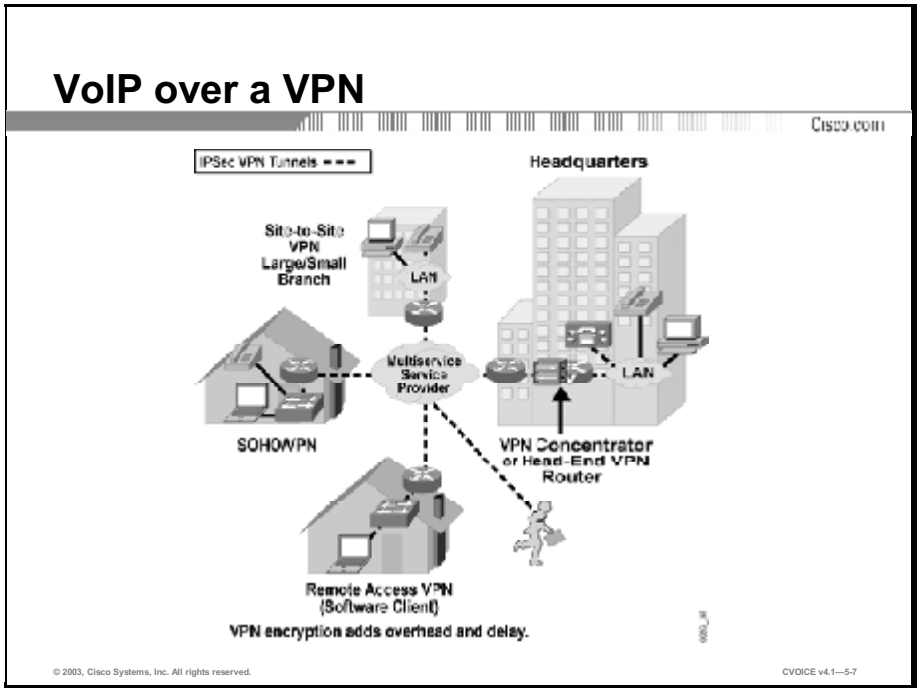
This table lists the ports used for various voice protocols.

Table 2: 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)	2427, 2727	UDP	MGCP gateway, MGCP call agent
Session Initiation Protocol (SIP)	5060	TCP or UDP	SIP call
Skinny	2000	TCP	Client
Skinny	2001	TCP	Digital gateway
Skinny	2002	TCP	Analog gateway
Skinny	2003	TCP	Conference bridge

Delivery of Voice over IP Through 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 impact 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, even with a modest amount of latency. 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.

Table 3: 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. The 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.

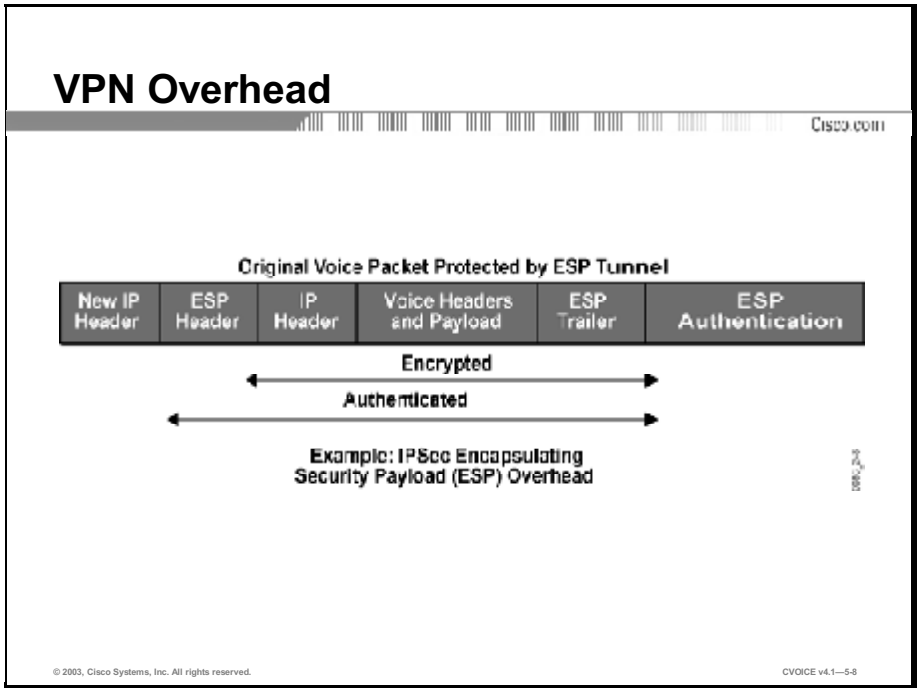
Overhead can be minimized if you understand the proper use of VPN technologies. VPNs can be implemented at Layer 2 through Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunnel Protocol (L2TP), as well as at Layer 3 with IPSec. Often Layer 2 and Layer 3 technologies are combined to provide additional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

International Issues

VoIP and either DES or 3DES encryption are fully compatible with each other, assuming that the VPN delivers the necessary throughput. Internationally, however, corporations can run into other factors. The U.S. Department of Commerce places restrictions on the export of certain encryption technology; DES is usually exportable, while 3DES is not. On the other hand, that generality takes numerous forms, from total export exclusions applied to a handful of countries to allowing 3DES export to specific industries and users. Most corporations whose VPNs 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 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 speaking, IPSec encrypts and/or authenticates 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:

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

Example

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

Table 4: VPN Packet

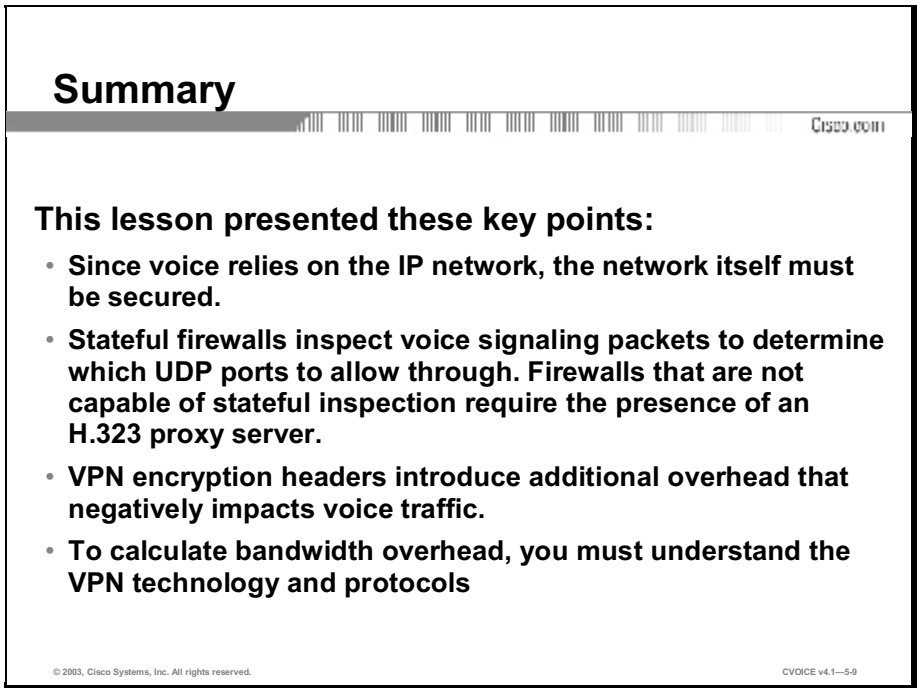
Field	Subhead
Voice payload (G.729)	20 bytes
RTP header	12 bytes
UDP header	8 bytes
IP header	20 bytes
VPN header	20 to 60 bytes
New IP header	20 bytes

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

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

- Total bandwidth = 160 * 8
- Total bandwidth = 1280 bits / 20 ms
- Total bandwidth = 64000 bps

Summary



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Security Implications
- Voice over IP Signaling and Call Control Module

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
- "RFC 2401 Security Architecture for the Internet Protocol" http://www.ietf.org/rfc/rfc2401.txt?number=2401

Quiz: Security Implications

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe three elements of a security policy that are necessary for a Voice over IP network
- Describe the dynamic access control process used by firewalls to allow voice packets to pass
- Outline the steps needed to reduce overhead and delay for Voice over IP in a VPN
- Describe how to calculate the bandwidth required for a VPN packet

Instructions

Answer these questions:

Q1) 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) all of the above

Q2) In which situation can the firewall inspect the packet for call setup?

A) when the firewall is configured for call setup

B) when the VPN terminates outside the firewall

C) when the VPN terminates inside the firewall

D) when the firewall does not recognize the signal or payload ports

Q3) 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

Q4) 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) all of the above

Q5) How does hardware encryption reduce overhead and delay as compared to software encryption?

A) It optimizes the encryption algorithm and data path.

B) It handles all processing in a dedicated encryption processor.

C) It does not rely on CPU resources.

D) It uses proper QoS technologies.

Q6) Which type of encryption technology may not be used on international networks because of government restrictions?

A) DES

B) 3DES

C) ESP

D) IPSec

Q7) How many bytes of overhead does VPN add to the voice packet?

A) 20 bytes

B) 40 bytes

C) 20 to 60 bytes

D) 40 to 80 bytes

Q8) Which type of VPN is most commonly used today?

A) IPSec

B) ESP

C) PPTP

D) L2TP

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

6

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).

Upon completing this module, you will be able to:

- Identify the appropriate call control model for your network, given the common control components and the pros and cons of the centralized and distributed call control models
- Configure, monitor, and troubleshoot H.323 gateways and gatekeepers, given the functions and capabilities of H.323 components in different call setup scenarios
- Configure, monitor, and troubleshoot SIP on a Cisco router, given the components and call setup methods of SIP
- Configure, monitor, and troubleshoot MGCP on a Cisco router, given the components and call setup procedures of MGCP
- Determine the best call control model for your network, given the requirements of your network and the characteristics and strengths of the H.323, SIP, and MGCP call control models

Outline

The module contains these topics:

- Need for Signaling and Call Control
- H.323
- SIP
- MGCP
- Comparing Call Control Models

Need for 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.

Importance

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:

- Describe the endpoints and the common control components that are used in VoIP signaling
- List five protocols used for call control in VoIP
- Explain why the call control gateway must translate signals from different call control models to support end-to-end calls
- List five call parameters that must be negotiated before placing a call
- Name the functions that are performed by call accounting and administration as common call control components

- Name the functions that are performed by call status and call detail records as common call control components
- Describe the address registration and address resolution functions that are performed by the address management common control component
- Explain how admission control can protect network resources when it is used as a common control component
- Illustrate the setup of a centralized call control model
- Illustrate the setup of a distributed call control model
- Identify the advantages and disadvantages of centralized and distributed call control

Learner Skills and Knowledge

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

- An understanding of the protocol environment in which VoIP operates.

Outline

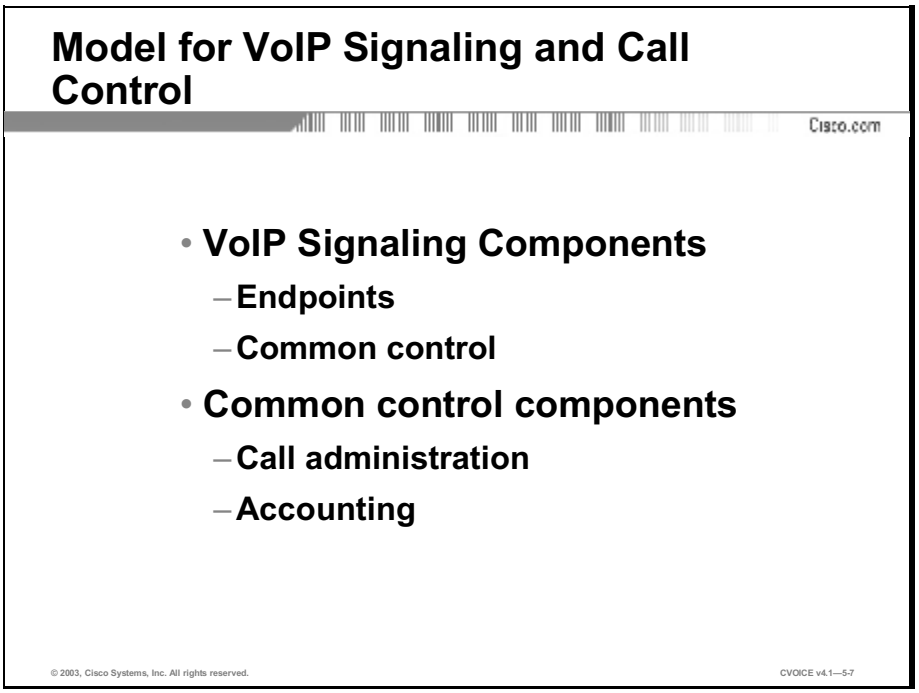
This lesson includes these topics:

- Overview
- VoIP Signaling
- Call Control Models
- Translation Between Signaling and Call Control Models
- Call Setup
- Call Administration and Accounting
- Call Status and Call Detail Records
- Address Management
- Admission Control
- Centralized Call Control
- Distributed Call Control

- Centralized Call Control vs. Distributed Call Control
- Summary
- Assessment (Quiz): Need for Signaling and Call Control

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 Voice over IP (VoIP) signaling.



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 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 the 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.

- **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.

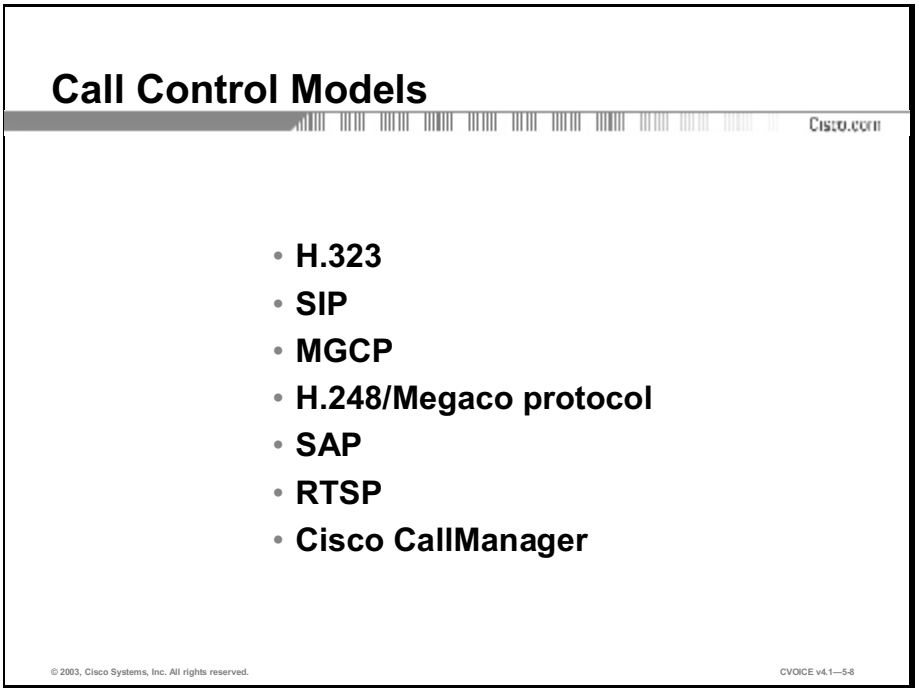
- **Common control:** In some call control models, the common control component is not defined; in others, it is employed optionally. Common control components provide call administration and accounting. These components provide a variety of services to support call establishment, including the following:

  - 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.



Several call control models and their corresponding protocols exist or are in development:

- **H.323:** International Telecommunication Union Telecommunication Standardization Sector (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 where 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).

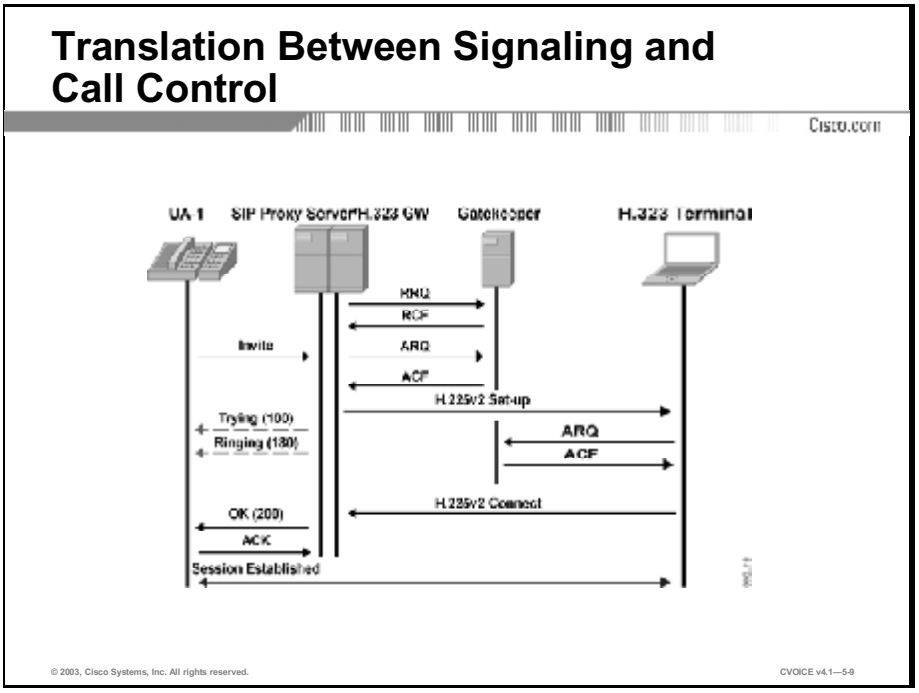
- **Session Announcement Protocol (SAP):** SAP (IETF RFC 2974) describes a multicast mechanism for advertising the session characteristics of a multimedia session, including audio and video.

- **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"):** 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 telephones, 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 the SIP protocol. However, it 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

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 include the following:

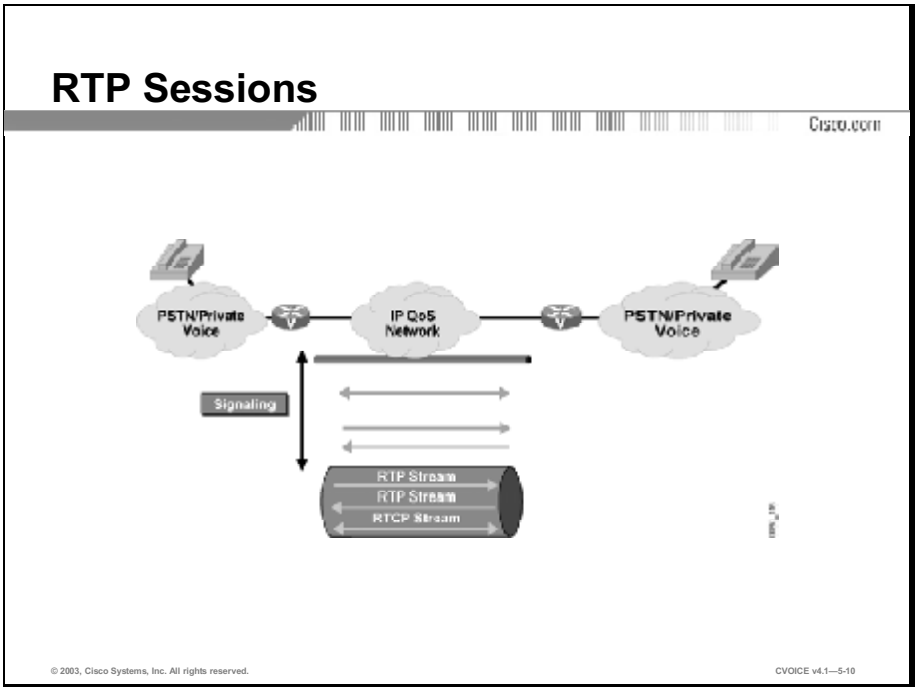
- Analog signaling (Foreign Exchange Station [FXS] or Foreign Exchange Office [FXO] loop start) to the CO
- CCSS7 between the COs,
- ISDN PRI signaling to the PBX
- Proprietary signaling to the desktop telephone

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 utilizes 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

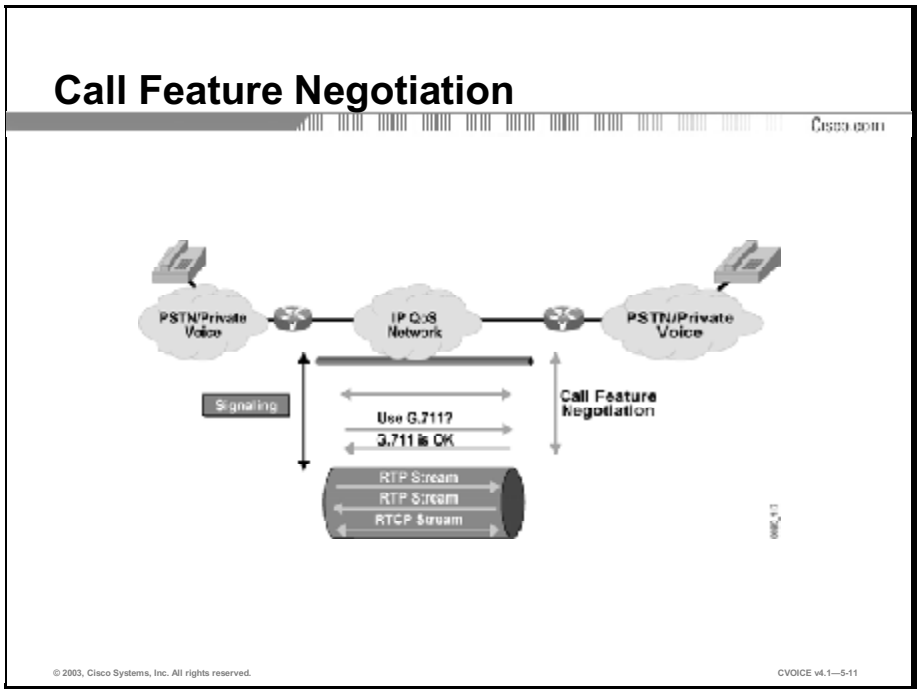
A fundamental objective of VoIP call control is to initiate communication between VoIP endpoints. This topic discusses the role of call control in establishing RTP sessions and negotiating features during the call setup procedure.



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.



Creating the RTP sessions is not the only task of call control during call setup. The endpoints need to establish a bilateral agreement where 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.

Some examples of call parameters are:

- **Coder-decoder (codec):** Each endpoint must share a common format for the voice, or at a minimum, 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/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 or transmit-only traffic when the call requests two-way communication.

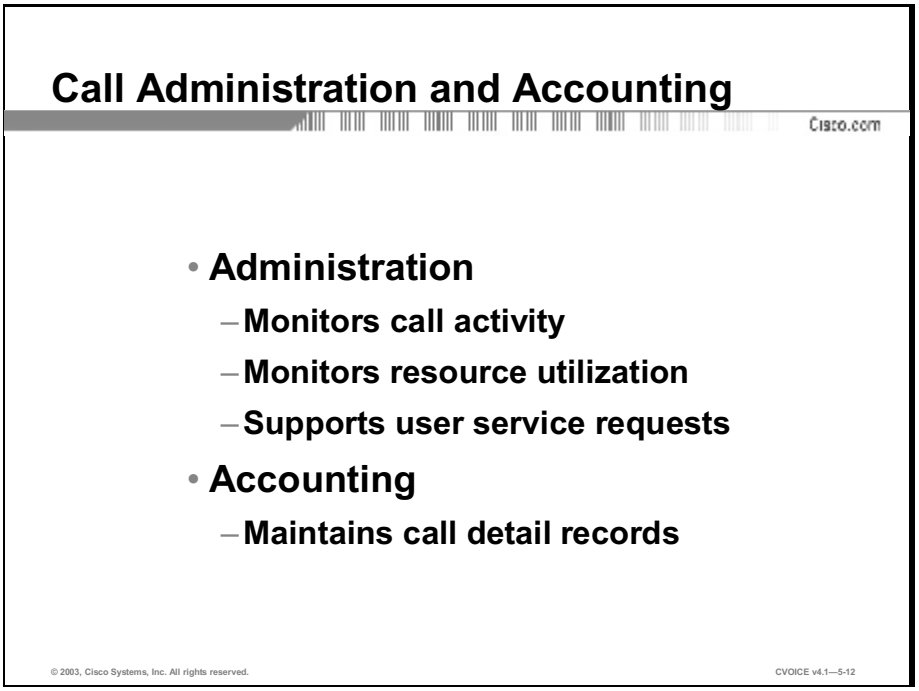
- **Multipoint conferences:** The type of conference and parameters to join.

- **Media type:** Audio, video, or data.

- **Bit rate:** Throughput requirements.

Call Administration and Accounting

Call control procedures typically provide support for call administration and accounting. This topic discusses these capabilities.



Call administration and accounting functions provide optional services for the improved operation, administration, and maintenance of a VoIP environment.

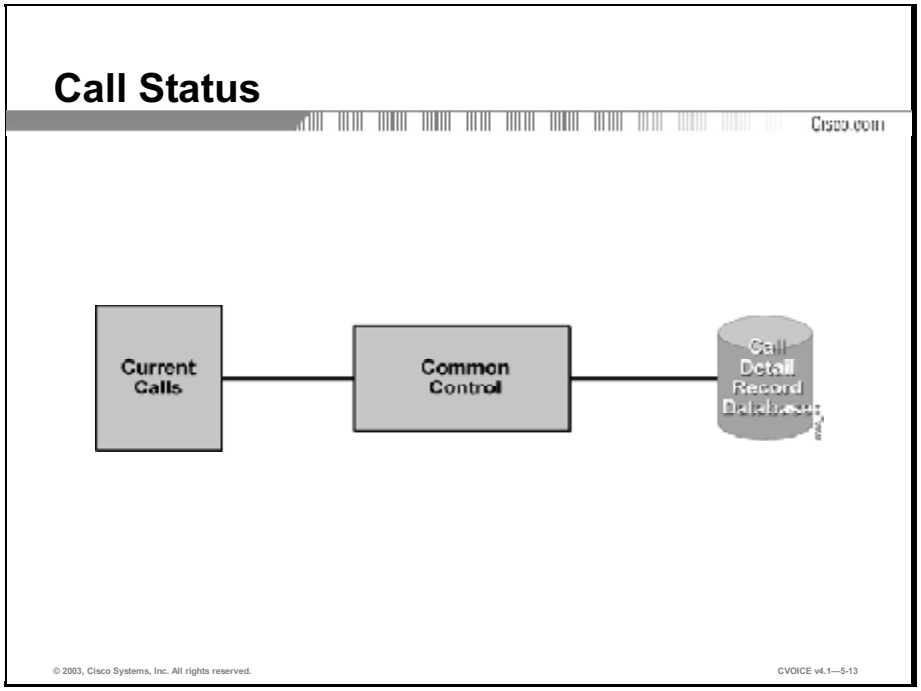
Accounting makes use of the historical information that is usually formatted as call detail records. Call detail records are useful for cost allocation and for determining call distribution and service grade for capacity-planning purposes.

Call administration includes the following 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 Call Detail Records

Several call control protocols offer dynamic access to the status of calls within the VoIP network. This topic discusses the benefits of maintaining call status information and describes where and how call status is used.



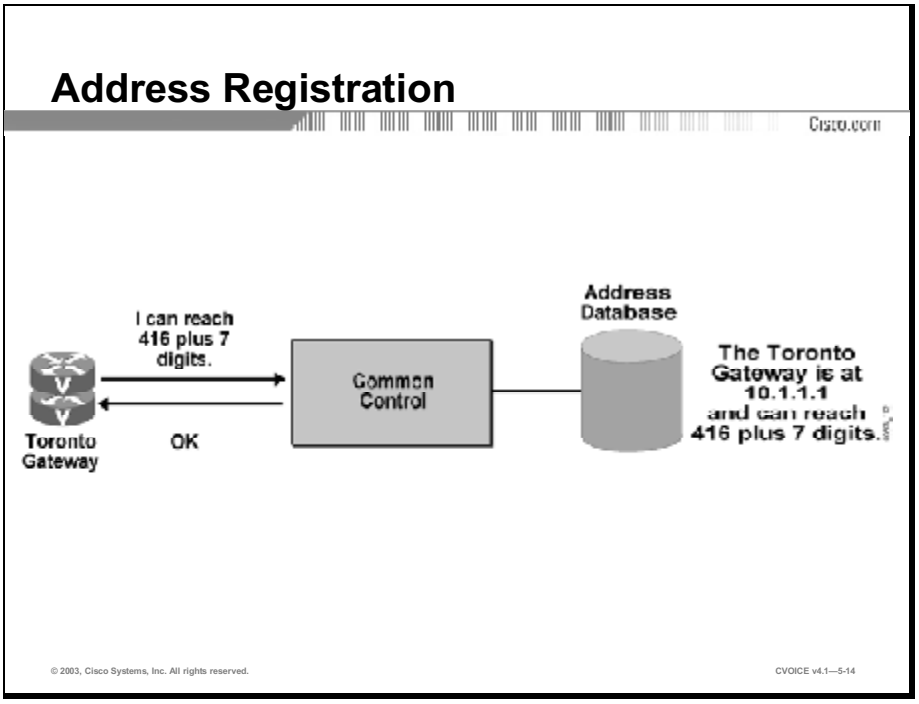
Several of the responsibilities that are assigned to call administration and accounting are dependent on access to current call status information or records of changes in the call status. Call status has both historical and instantaneous (real-time) benefits. Call detail records have consequential benefits 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.

Call detail records 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 topic discusses how endpoints register their addresses and how these addresses are resolved to IP addresses.

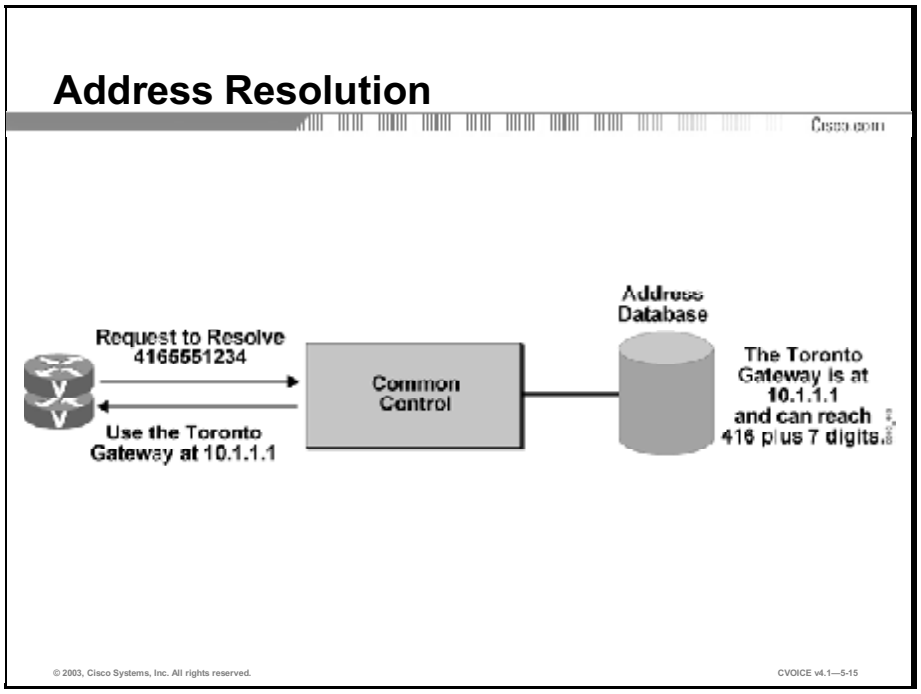


When an endpoint registers with a call control component, it supplies its telephone address or addresses and, if it is a gateway, the addresses of the destinations it can reach. The endpoint provides other information relating to its capabilities. Multiple destinations that are reachable through a gateway 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

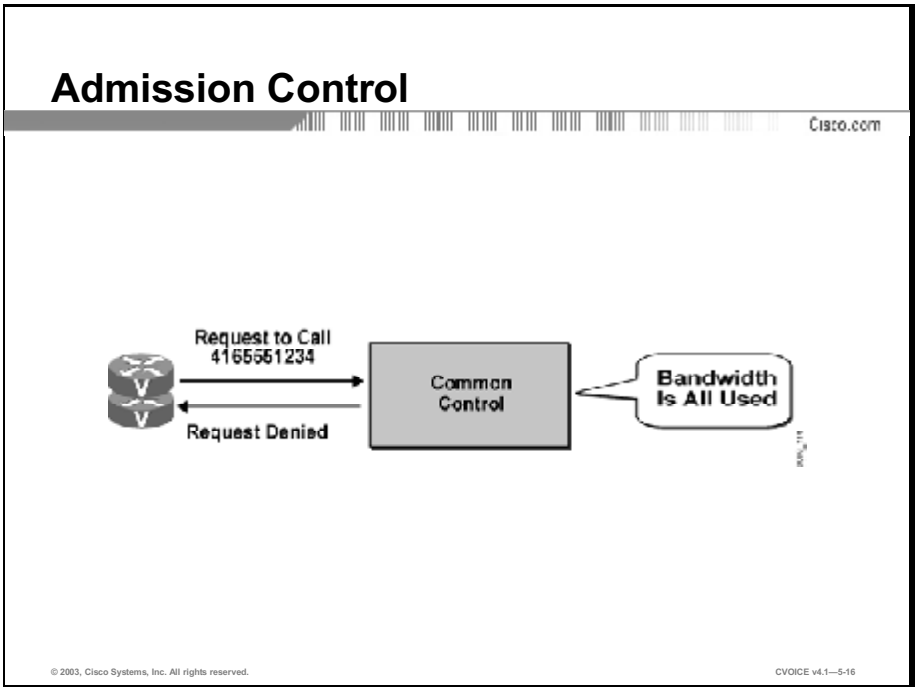
The figure illustrates the Toronto gateway registering its accessibility information. In this example, the gateway informs the common control component that it can reach all telephone numbers in the 416 area. This information is deposited into a database for future reference.



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 topic discusses how common control and bandwidth management restrict access to the network.



Admission control has at least two aspects: authorization and bandwidth management.

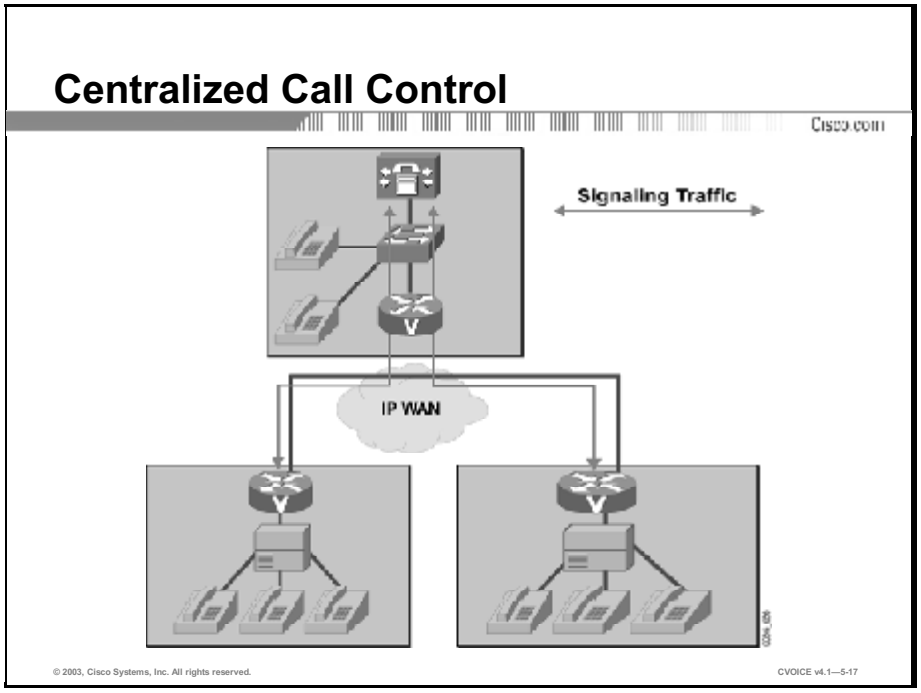
Access to a network should not imply permission to use the resources of the network. Common control limits access to the resources by checking the intentions and credentials of users before authorizing them to proceed.

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 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.

Centralized Call Control

This topic describes the function of endpoints in a centralized call control model.



The level of "intelligence" associated with an endpoint classifies call control models. In centralized call control, the intelligence in the network is associated with one or several controllers. Endpoints provide physical interconnection to the telephone network; however, they still require the central controller to dictate when and how to use their interconnect capability. For example, the central controller may require the endpoint to provide dial tone to a telephone and alert the controller when a telephone goes off hook. The endpoint *does not* make decisions autonomously.

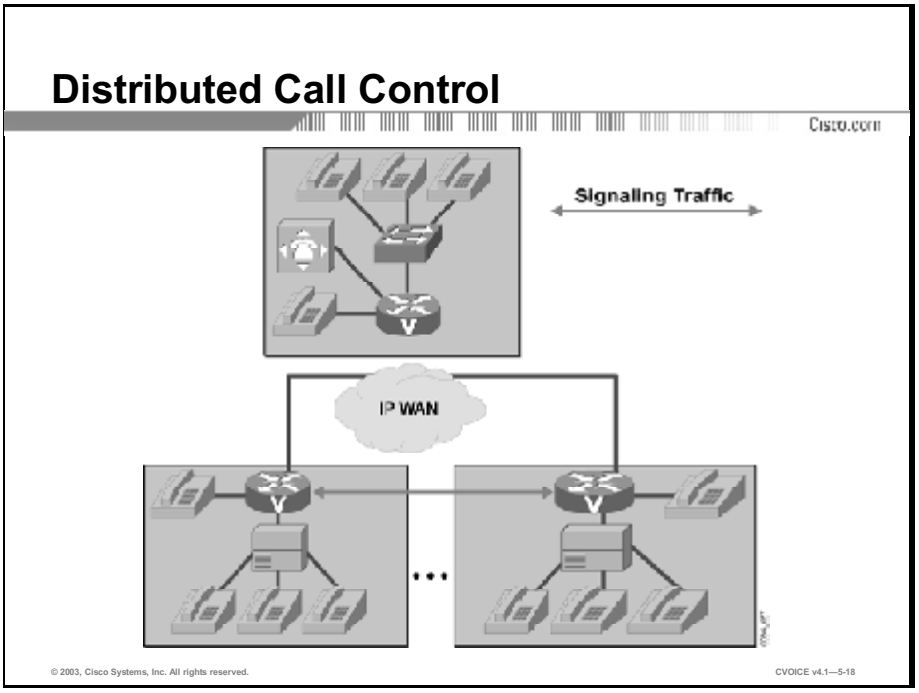
Example

The figure illustrates two gateways interacting with a centralized call control component for call setup and management. Notice that the media path is between the two gateways.

A centralized call control model is similar to the mainframe model of computing and uses centralized common control concepts that are found in circuit-switching solutions.

Distributed Call Control

This topic describes the functions of the endpoints in a distributed call control model.



Endpoints in a distributed call control model have sufficient intelligence to autonomously manage the telephone interface and initiate VoIP call setup. Although the endpoint in a distributed model often depends on shared common control components for scalability, it possesses enough intelligence to operate independently from the common control components. If a common control component fails, an endpoint can use its own capabilities and resources to make routing or rerouting decisions.

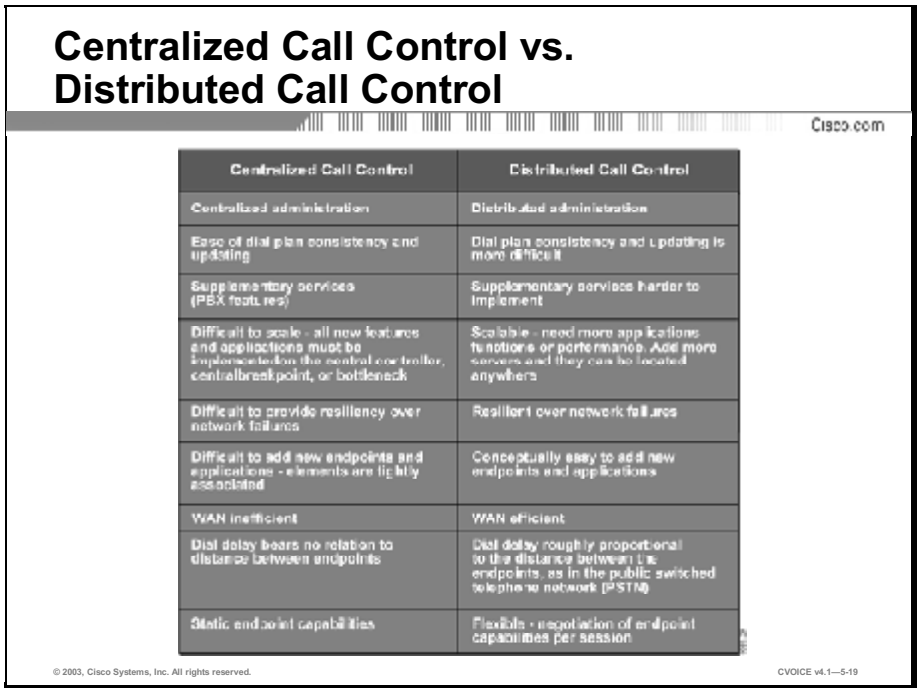
Example

In the figure, the two gateways have established a call control path and a media path between themselves, without the assistance of a centralized call control component.

A distributed call model is analogous to a desktop computing model.

Centralized Call Control vs. Distributed Call Control

This topic compares the advantages and disadvantages of the centralized and distributed call control models.



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 are disadvantages of the other type. The main differences between the two models are in the following 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 and provides a convenient location for the collection and dissemination of call detail records. The distributed model requires distributed administration of the configuration and management of endpoints, thus complicating the administration of a dial plan. Although distributed call control simplifies the deployment of additional endpoints, new features and supplementary services are difficult to implement.

- **Security:** Centralized call control requires that endpoints are known to a central authority, which avoids (or at least reduces), security concerns. The autonomy of endpoints in the distributed model elevates security concerns.

- **Reliability:** The centralized model is vulnerable because of its single point-of-failure and contention. It 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, thus reducing vulnerability.

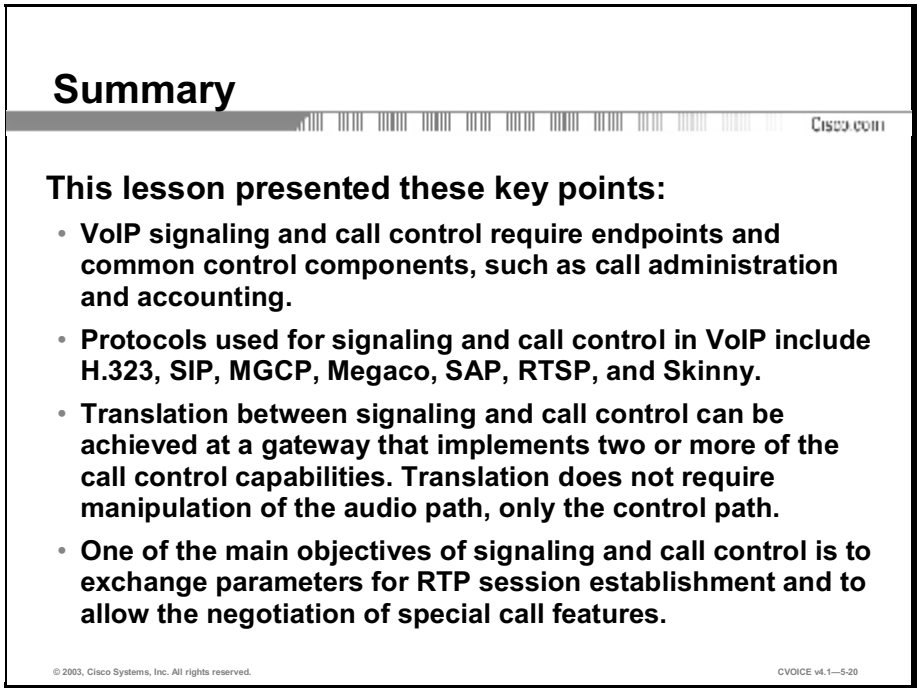
- **Efficiency:** Centralized call control fails to take full advantage of computer-based technology that resides in the endpoints. It also consumes bandwidth through the interaction of the call agent and its endpoints. Distributed call control takes advantage of the inherent computer-based technology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

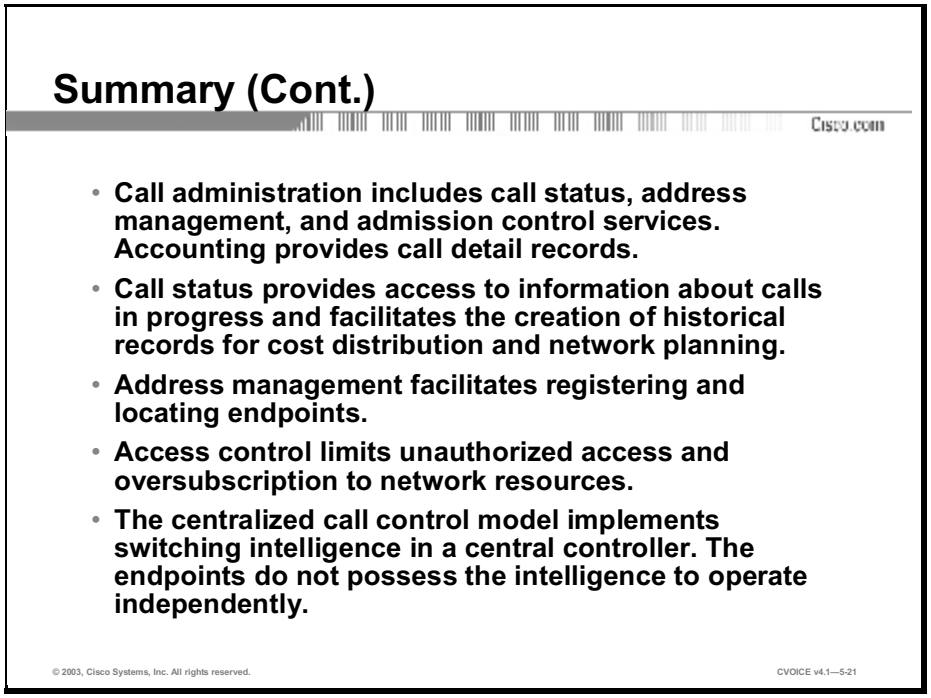
Example

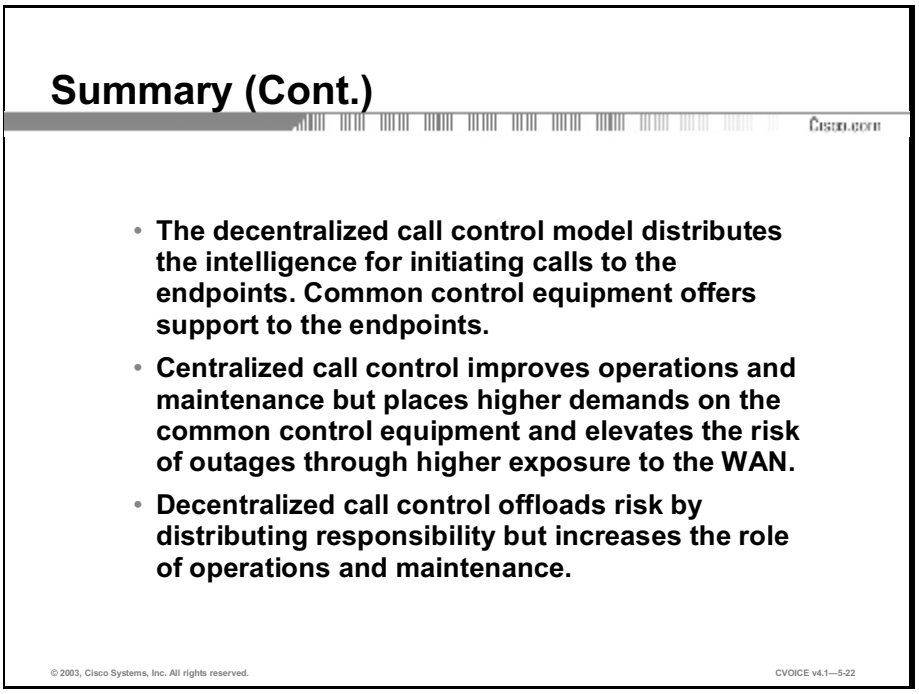
Because the centralized model increases vulnerability, it mandates the implementation of survivability and load management strategies that involve the replication of the central components. Few implementations of call control are totally distributed. For example, although H.323 and session initiation protocol (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.

Summary

This topic summarizes the key points discussed in this lesson.







Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Need for Signaling and Call Control
- H.323 lesson

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”

Quiz: Need for Signaling and Call Control

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the endpoints and the common control components that are used in VoIP signaling
- List five protocols that are used for call control in VoIP
- Explain why the call control gateway must translate signals from different call control models to support end-to-end calls
- List five call parameters that must be negotiated before placing a call
- Name the functions that are performed by call accounting and administration as common call control components
- Name the functions that are performed by call status and call detail records as common call control components
- Describe the address registration and address resolution functions that are performed by the address management common control component
- Explain how admission control can protect network resources when it is used as a common control component
- Illustrate the setup of a centralized call control model
- Illustrate the setup of a distributed call control model
- Identify the advantages and disadvantages of centralized and distributed call control

Instructions

Answer these questions:

Q1) What are two examples of signaling systems that are used in traditional telephony? (Choose two.)

A) red-light signaling

B) YBTM Signaling

C) Common Channel Signaling System 7

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) Which protocol is NOT an example of a VoIP call control model?

A) SIP

B) RSVP

C) Megaco

D) SAP

Q4) Match the call control model with its description.

A) H.323

B) MGCP

C) H.248

D) RTSP

E) Skinny

_____ 1. describes 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) Which call control function is required at the gateway to allow two endpoints using different call control models to communicate?

A) authentication

B) compression

C) registration

D) translation

Q7) Which two of the following 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) To create RTP sessions, which information does each endpoint need to recognize?

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) call detail records

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) call detail records

_____ 1. ensures 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 call detail records? (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 call detail records

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 it can reach?

A) a list of all the telephone numbers it can reach

B) a list of all the IP addresses it can reach

C) a routing table

D) a prefix

Q15) What are two aspects of admission control? (Choose two.)

A) authentication

B) authorization

C) call detail record creation

D) bandwidth management

E) address resolution

Q16) What information do the bandwidth management and call admission control functions use to monitor bandwidth consumption?

A) router configuration

B) network speed

C) call detail records

D) call status data

Q17) Which device has the most intelligence in a centralized call control model?

A) originating endpoint

B) central controller

C) gateway

D) gatekeeper

E) intermediate router

Q18) Which statements regarding endpoints are true in a centralized call control model?

A) Endpoints automatically provide dial tone when a telephone goes off hook.

B) Endpoints automatically start call setup when a telephone goes off hook.

C) Endpoints manage calls that are in progress.

D) Endpoints provide physical connections for the telephone network.

E) Endpoints decide when and how to use their interconnect abilities.

Q19) Which capability of a distributed call control model endpoint is the same as a centralized call control endpoint?

A) Endpoints manage the telephone interface.

B) Endpoints autonomously initiate call setup.

C) Endpoints route calls in case a common control component fails.

D) Endpoints have a media path between them.

Q20) What may be one reason for endpoints to share common control components in a distributed call control model?

A) bandwidth conservation

B) scalability

C) ease of call setup

D) faster routing

Q21) What are two advantages of a distributed call control model? (Choose two.)

A) It provides superior configuration control.

B) It provides fault tolerance.

C) It simplifies introduction of new features.

D) It simplifies deployment of additional endpoints.

E) It provides superior maintenance of the endpoint database.

Q22) What are two advantages of a centralized call control model? (Choose two.)

A) It minimizes dependence on network resources.

B) It provides superior maintenance of the dial plan.

C) It simplifies introduction of supplementary services.

D) It simplifies deployment of additional endpoints.

E) It reduces bandwidth consumption.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

H.323

Overview

H.323 and its associated International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendations represent a distributed environment for establishing voice, video, and data communication in a non-guaranteed 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.

Importance

An understanding of the features and functions of H.323, its components, and the manner in which the components interface is important to implement a scalable, resilient, and secure H.323 environment.

Objectives

Upon completing this lesson, you will be able to:

- Describe the recommendations that are associated with H.323 and the control and signaling functions they perform
- List the functions that are performed by the components of 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

- Describe three types of multipoint conferences that are supported by H.323
- Provide a scenario of call flow with multiple gatekeepers and explain how this allows scalability
- Describe four strategies that are used by H.323 to provide fault tolerance networks
- List the steps involved in using an H.323 proxy server to set up end-to-end connections
- List the components that are supported by the Cisco Systems implementation of H.323
- Use the commands that are required to configure gateways in a two-zone, two-gatekeeper scenario
- Use the commands that are required to configure gatekeepers in a two-zone, two-gatekeeper scenario
- List the **show** and **debug** commands that are used to monitor and troubleshoot Cisco H.323 gateways and gatekeepers

Learner Skills and Knowledge

To fully benefit 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 Voice over IP (VoIP)

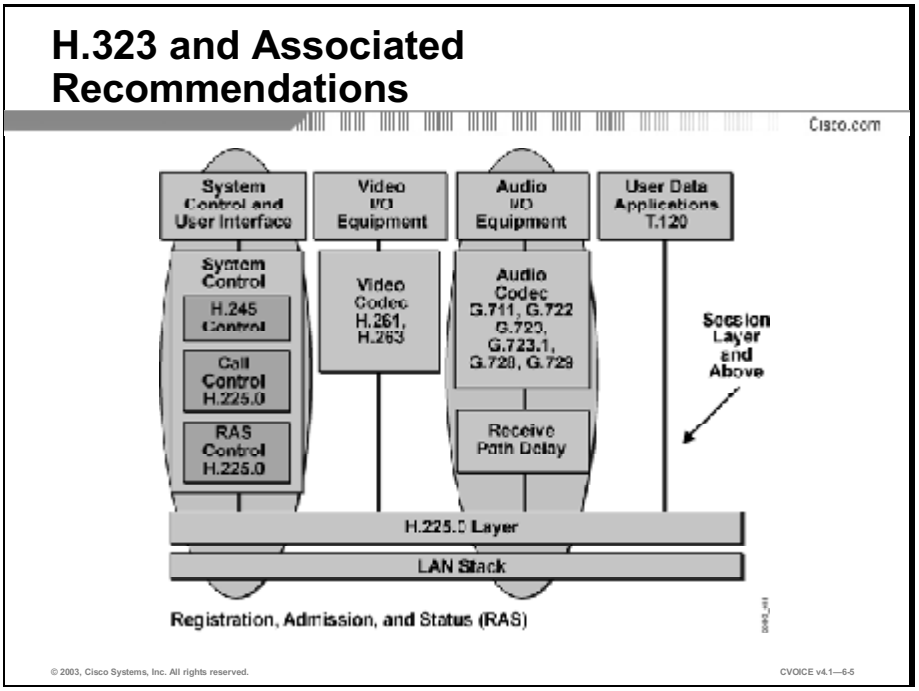
Outline

This lesson includes these topics:

- Overview
- H.323 and Associated Recommendations
- Functional Components of H.323
- H.323 Call Establishment and Maintenance
- Call Flows Without a Gatekeeper
- Call Flows with a Gatekeeper
- Multipoint Conferences
- Call Flows with Multiple Gatekeepers
- Survivability Strategies
- H.323 Proxy Server
- Cisco Implementation of H.323
- Configuring H.323 Gateways
- Configuring H.323 Gatekeepers
- Monitoring and Troubleshooting
- Summary
- Assessment (Quiz): H.323
- Assessment (Complex Lab): Lab Exercise 6-1

H.323 and Associated Recommendations

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 Voice over IP (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 the following protocols:

- H.245 for capabilities exchange
- H.225.0 for call setup
- H.225.0 for registration, admission, and status (RAS) control for call routing

H.323 is based on the 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. Following is a description of these functions.

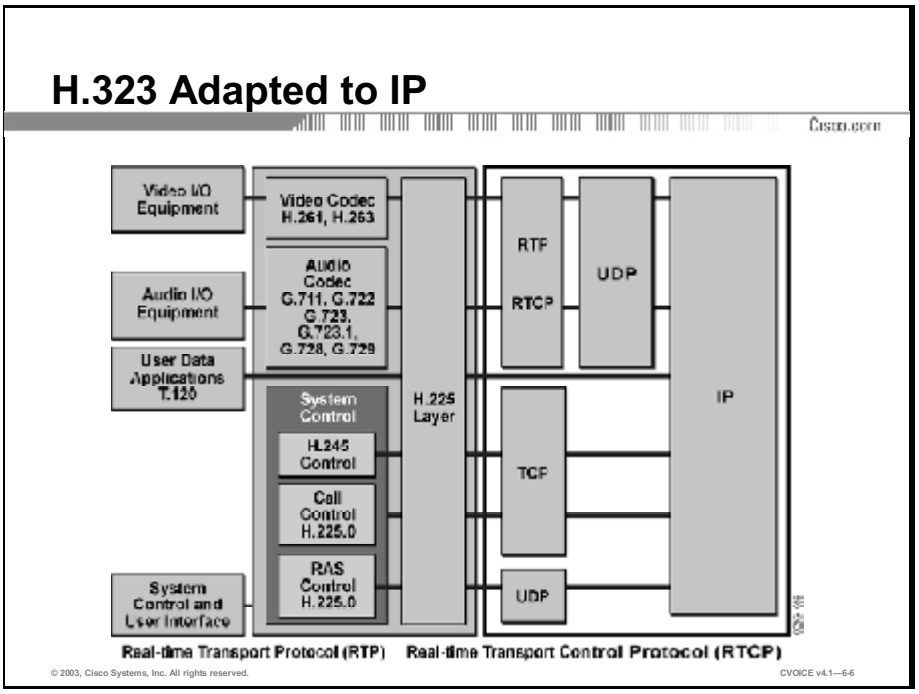
- **Call signaling function:** The call signaling function uses a call signaling channel that allows an endpoint to create connections with other endpoints. The call signaling function defines call setup procedures, based on the call setup procedures for ISDN (Recommendation Q.931). The call signaling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

  - **Logical channel signaling:** Opens and closes the channel that carries the media stream.
  - **Capabilities exchange:** Negotiates audio, video, and codec capability between the endpoints.
  - **Master/slave determination:** Determines which endpoint is master and which is slave. 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.

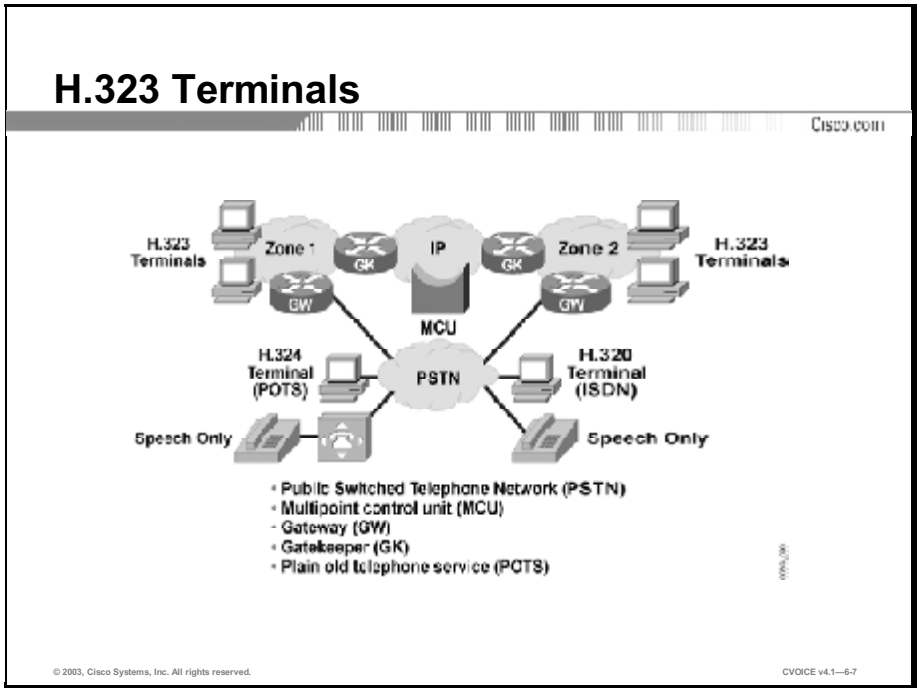


Example

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.

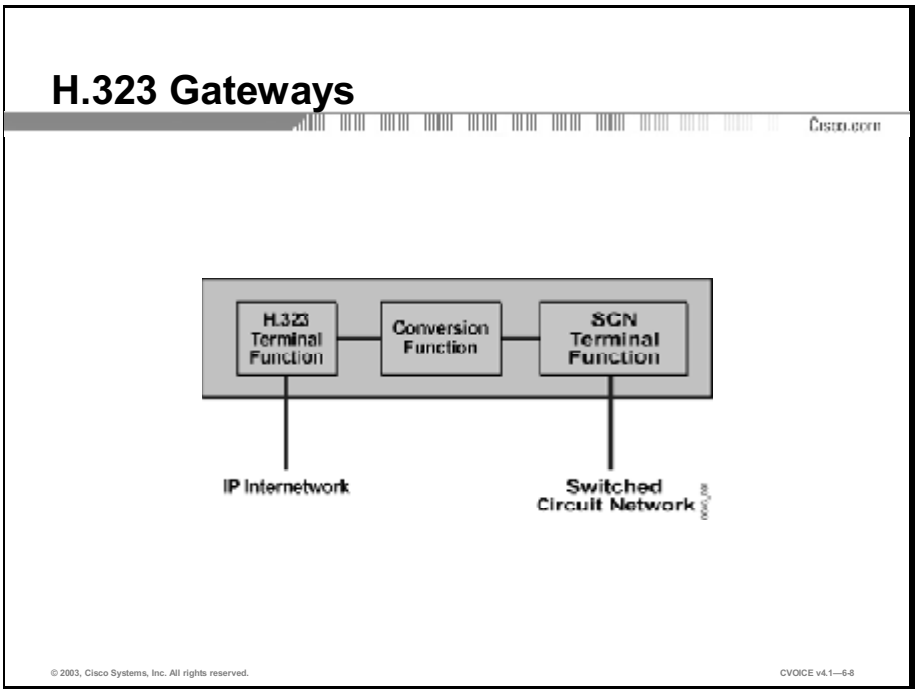
Functional Components of H.323

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, gateway, or multipoint control unit.

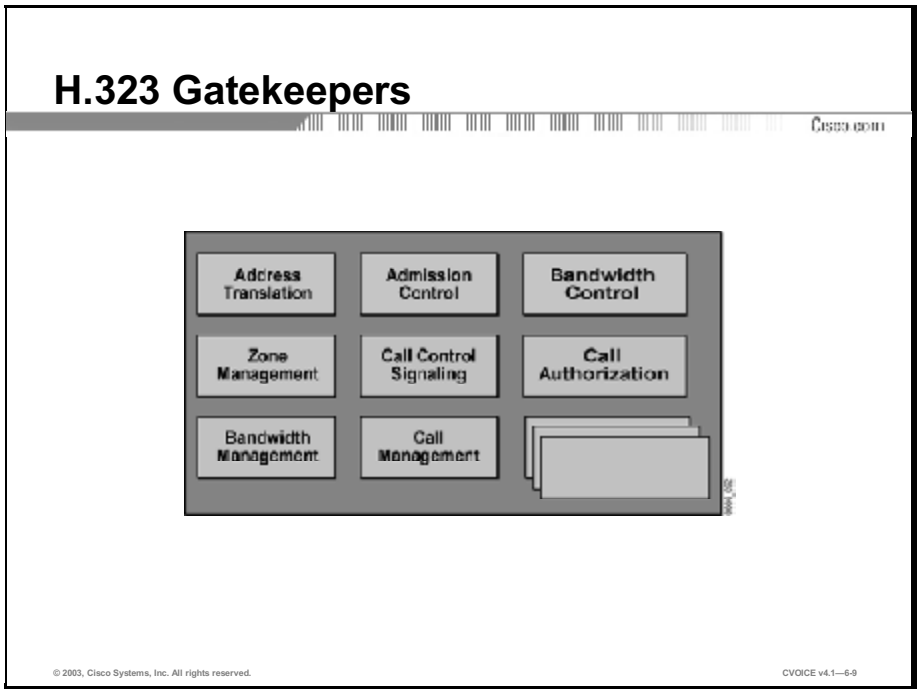
An H.323 terminal must be capable of transmitting and receiving G.711 (α-law and μ-law) 64-kbps pulse code modulation (PCM) encoded voice, and may support other encoded voice formats, such as G.729 and G.723.1.



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 the following services:

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



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 component, it can be colocated with any other H.323 component.

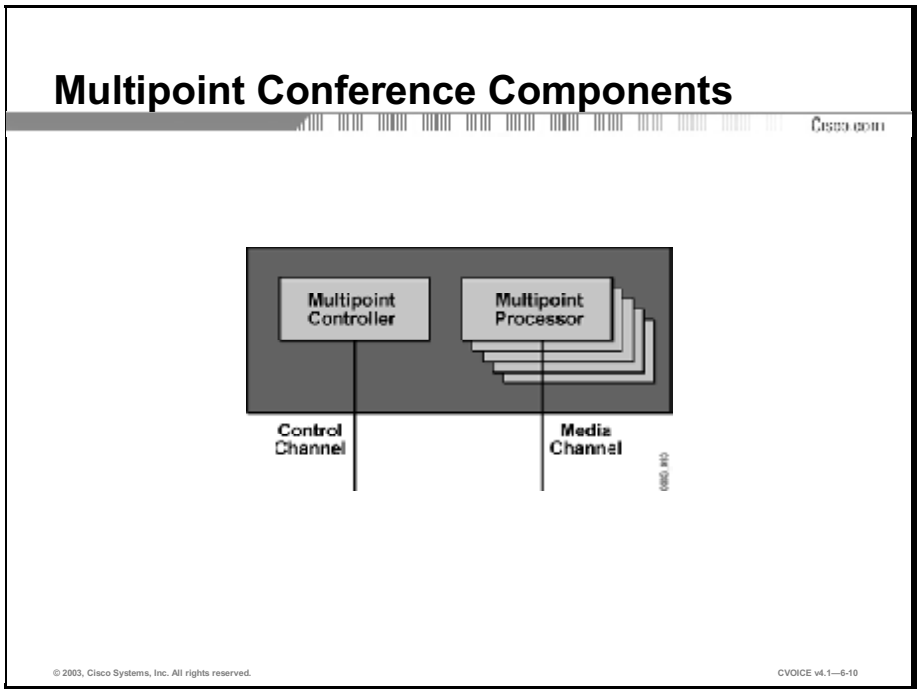
The scope of endpoints over which a gatekeeper exercises its authority is called a “zone.” H.323 defines a one-to-one relationship between a zone and a gatekeeper.

When a gatekeeper is included, it must perform the following 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:

- **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 (call admission control)
- **Call management:** Maintains a record of ongoing calls



Support for multipoint conferences is provided by the following three functional components.

- **Multipoint controller:** A multipoint controller (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 a multipoint control unit.

- **Multipoint processor:** A multipoint processor (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.

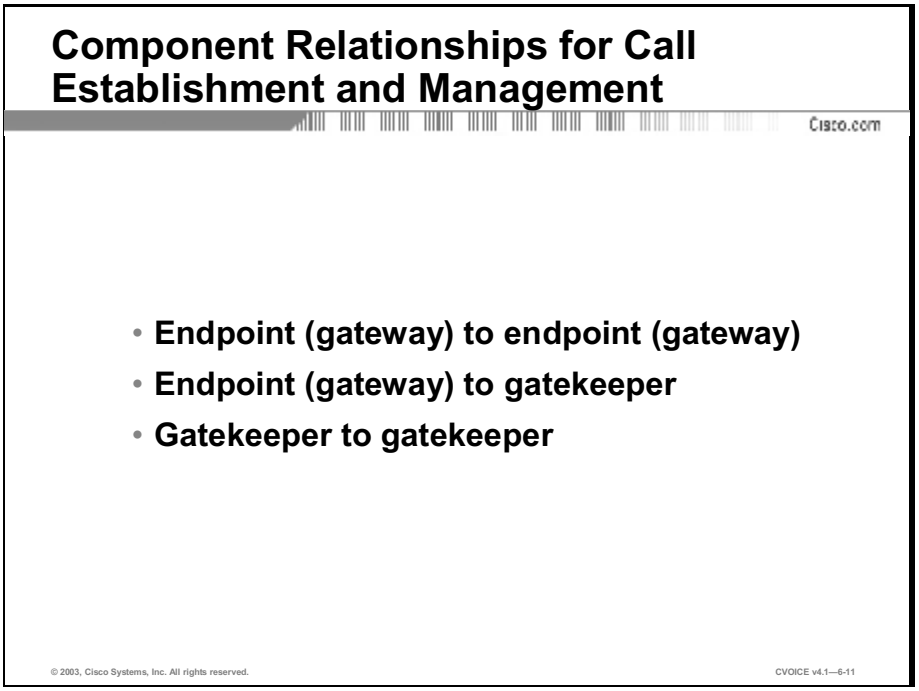
  Similar to an MC, an MP is not modeled as a standalone component; it resides in an MCU.

- **Multipoint control unit:** A multipoint control unit (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.

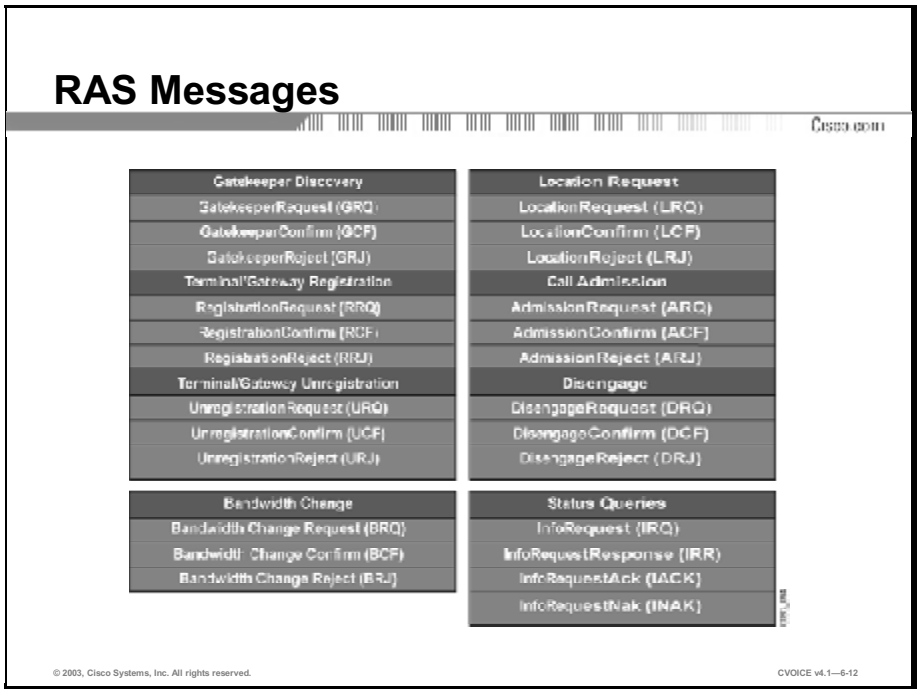
H.323 Call Establishment and Maintenance

This topic describes possible component scenarios required to establish end-to-end connections and the commands used by the components to establish VoIP calls.



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 the following 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.



Gatekeepers communicate through the RAS channel using different types of RAS messages. These message types include the following:

- **Gatekeeper discovery:** An endpoint multicasts a gatekeeper discovery request (GRQ). A gatekeeper may confirm (GCF) or reject (GRJ) an endpoint.

- **Terminal/gateway registration:** An endpoint sends a registration request (RRQ) to its gatekeeper to register and provide reachable prefixes. A gatekeeper confirms (RCF) or rejects (RRJ) the registration.

- **Terminal/gateway unregistration:** An endpoint or gatekeeper sends an "unregistration" request (URQ) to cancel a registration. The responding device confirms (UCF) or rejects (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 (LCF) with the IP address of the endpoint or rejects the request (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 (ACF) with the IP address of the terminating endpoint or rejects (ARJ) if the endpoint is unknown or inadequate bandwidth is available.

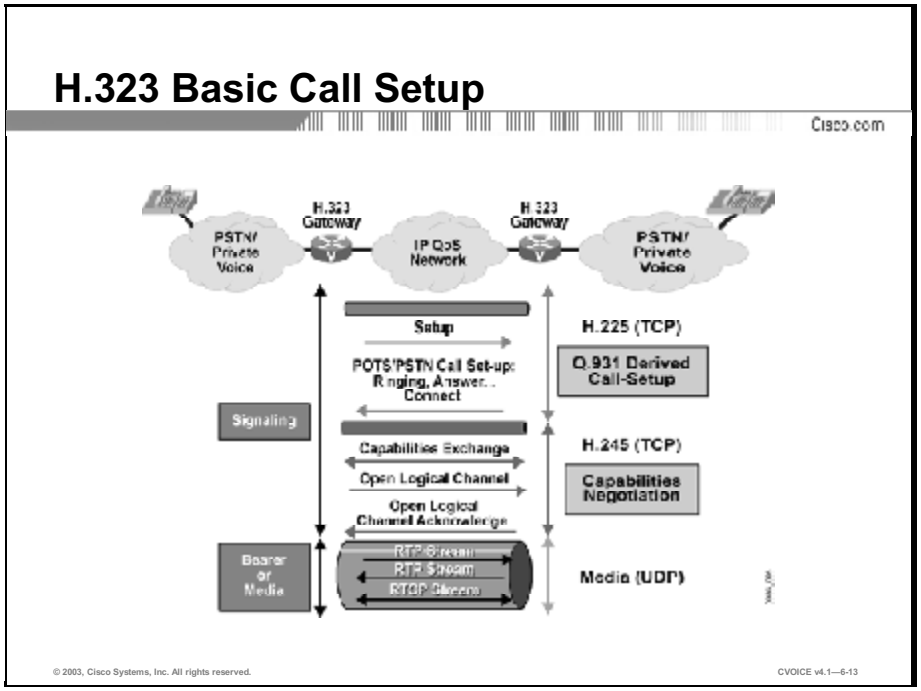
- **Bandwidth change:** An endpoint sends a bandwidth change request (BRQ) to its gatekeeper to request an adjustment in call bandwidth. A gatekeeper confirms (BCF) or rejects (BRJ) the request.

- **Disengage:** When a call is disconnected, the endpoint sends a disengage request (DRQ) to the gatekeeper. The gatekeeper confirms (DCF) or rejects (DRJ) the request.

- **Status queries:** A gatekeeper uses status request (IRQ) to determine the status of an endpoint. In its response (IRR), the endpoint indicates whether it is online or offline. The endpoint may also reply that it understands the information request (IACK) or that it does not understand the request (INAK).

Call Flows Without a Gatekeeper

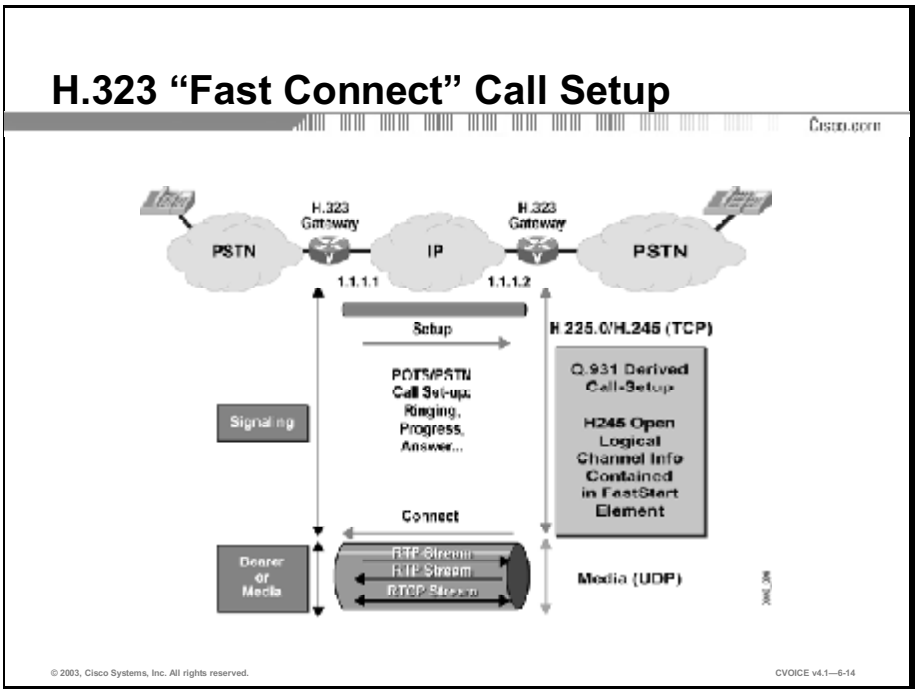
This topic describes call setup scenarios without a gatekeeper and provides examples of actual call flow procedures.



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 an H.323 terminal.

The flow procedure with 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 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.

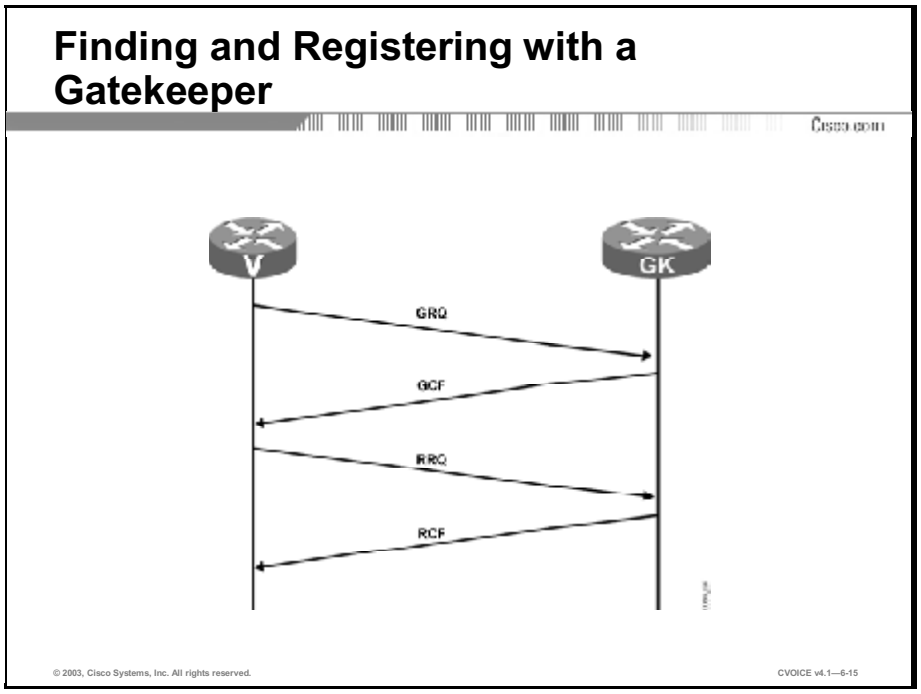


The figure shows an H.323 setup exchange that uses the "fast connect" abbreviated procedure available in version 2 of Recommendation H.323. The fast-connect procedure reduces the number of round-trip exchanges and achieves the capability exchange and logical channel assignments in one round trip.

The fast-connect procedure includes these steps:

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.

Reference Refer to Recommendation H.323 for a more complete set of call setup scenarios.



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 two methods are 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.

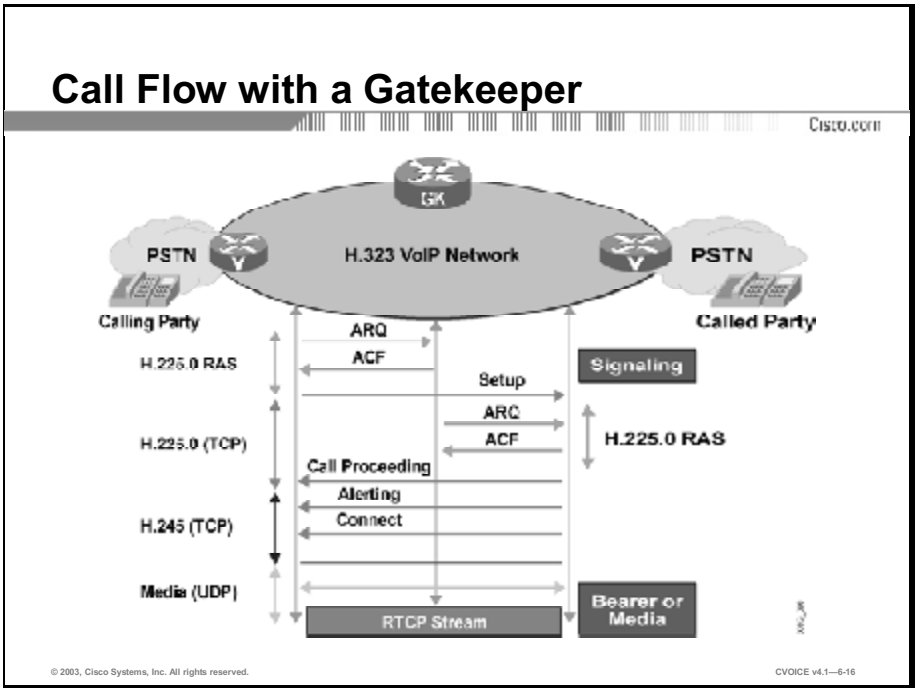
- An endpoint can issue a multicast GRQ to the gatekeeper discovery address (224.0.1.41) to discover the IP address of its gatekeeper. If the endpoint receives a GCF to the discovery, it uses the IP address to proceed with registration.

To initiate registration, an endpoint sends an RRQ to the gatekeeper. In the register request, 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 POTS dial-peer destination patterns associated with any FXS port.

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

Call Flows with a Gatekeeper

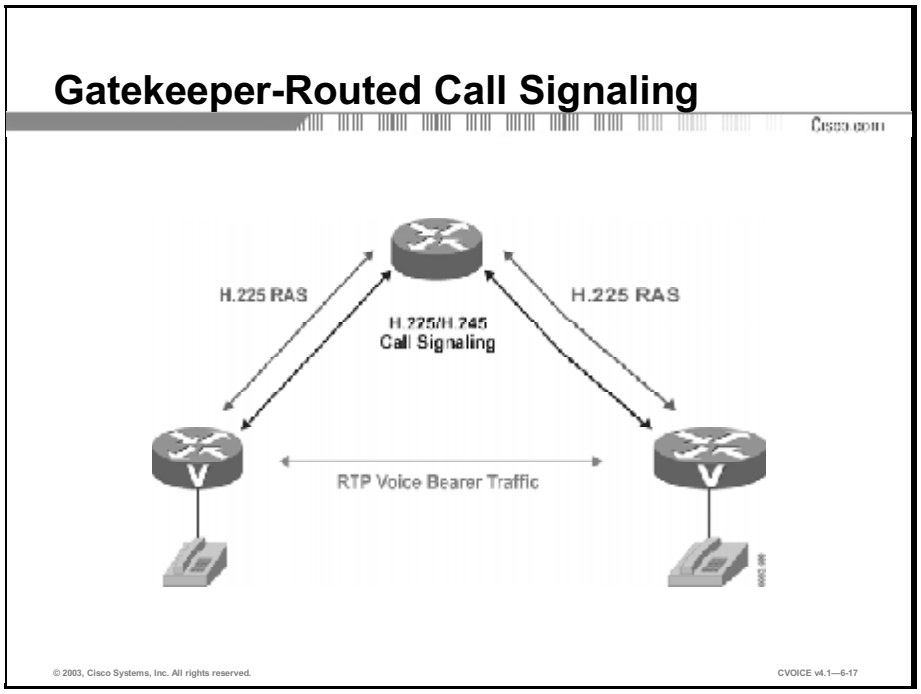
The topic discusses call setup scenarios with a gatekeeper.



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 admission request 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 admission request 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 admission request, the endpoint that receives the rejection terminates the procedure.

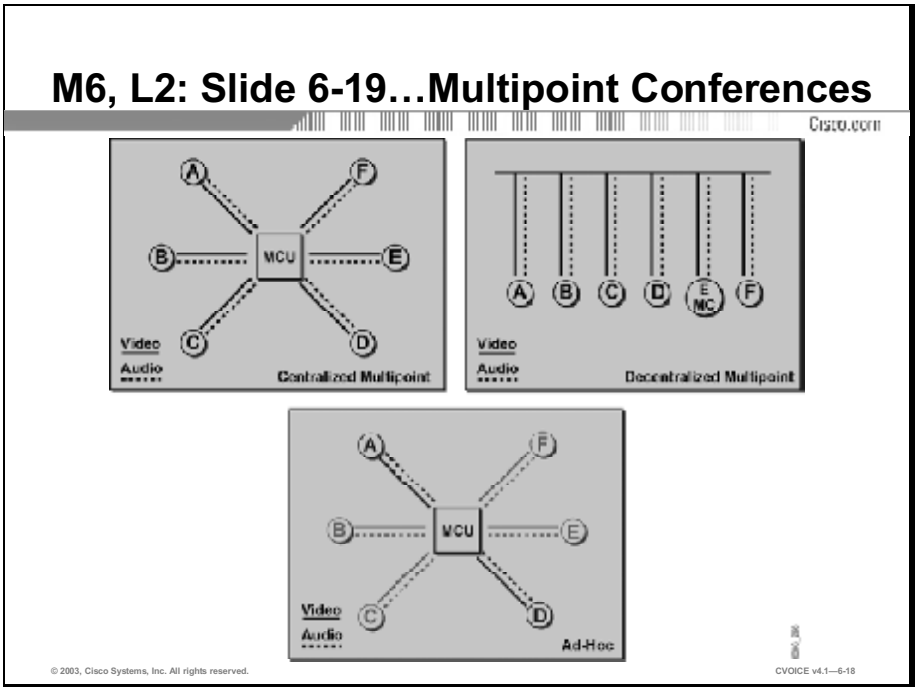


In the examples offered thus far, the call-signaling channel is created from endpoint to endpoint. In some cases, it is desirable to have the gatekeeper represent the other endpoint for signaling purposes. This method is called gatekeeper-routed call signaling. The process for gatekeeper-routed call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

1. The gatekeeper responds to an admission request 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 to the originating endpoint.
5. The two endpoints establish an H.245 control channel between them. The call procedure continues normally from this point.

Multipoint Conferences

H.323 defines three types of conferences—centralized multipoint, distributed multipoint, and ad-hoc multipoint. 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 Multipoint Controller (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 Multipoint Processor (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.

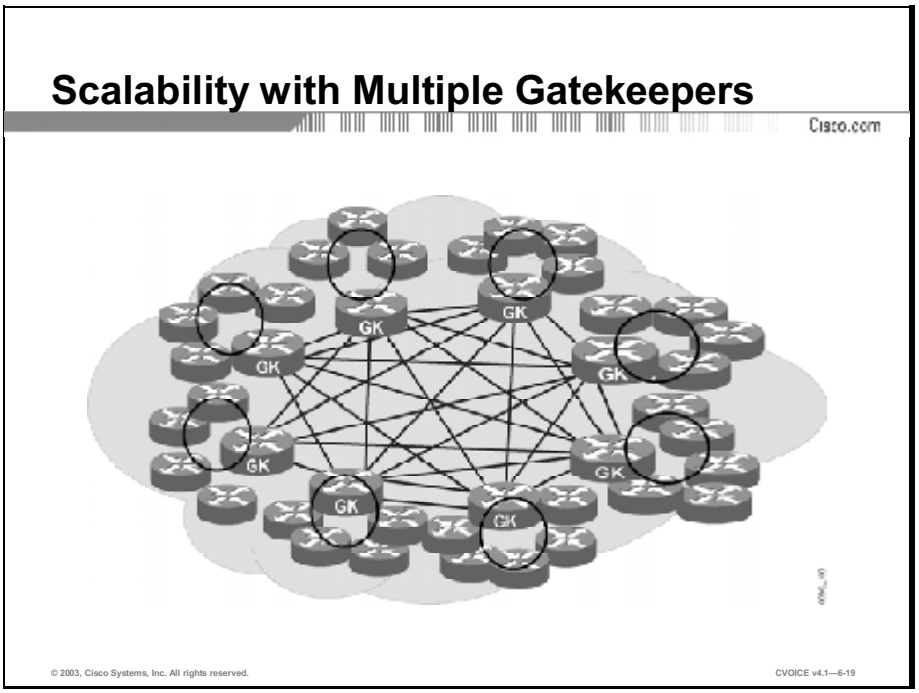
- **Distributed multipoint conference:** The endpoints do not have a connection to an MP. Instead, endpoints multicast their audio, video, and data streams to all participants in the conference. Because an MP is not available for switching and mixing, any mixing of the conference streams is a function of the endpoint, and all endpoints must use the same communication parameters.

To accommodate situations where two streams (audio and video) would be handled by the different multipoint conference models, H.323 defines a “hybrid.” A hybrid describes a situation where 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, then 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.

Call Flows with Multiple Gatekeepers

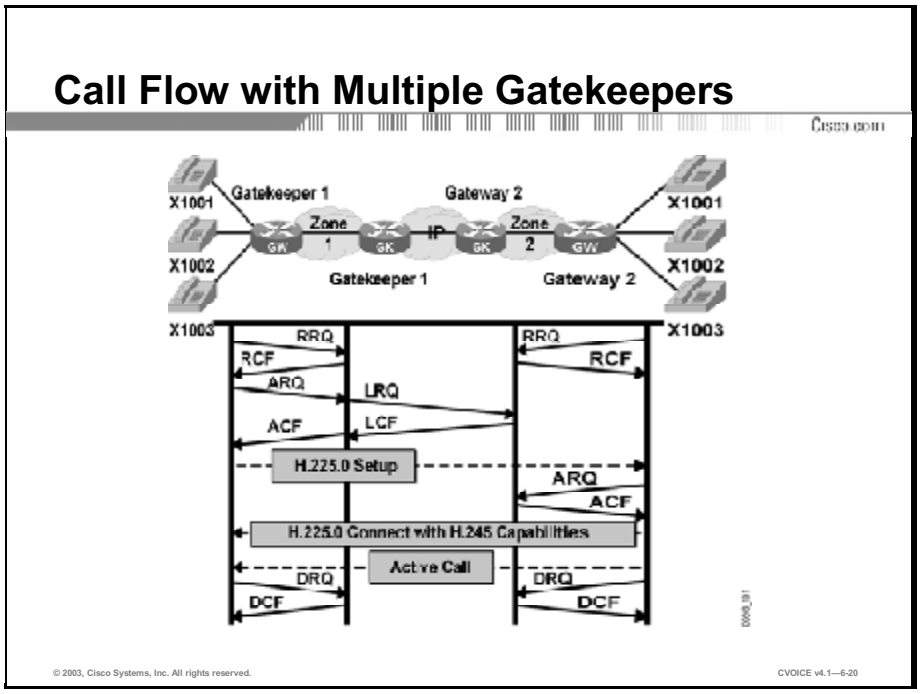
By simplifying configuration of the endpoints, gatekeepers aid in building large-scale VoIP networks. As the VoIP network grows, incorporating additional gatekeepers enhances the network scalability. This topic discusses the use of multiple gatekeepers for scalability and illustrates call flow in a multiple 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. There are vulnerability issues: a single gatekeeper can become overloaded or have an inconvenient network location, necessitating a long and expensive round trip to it.

Deploying multiple gatekeepers offers a more scalable and robust environment.

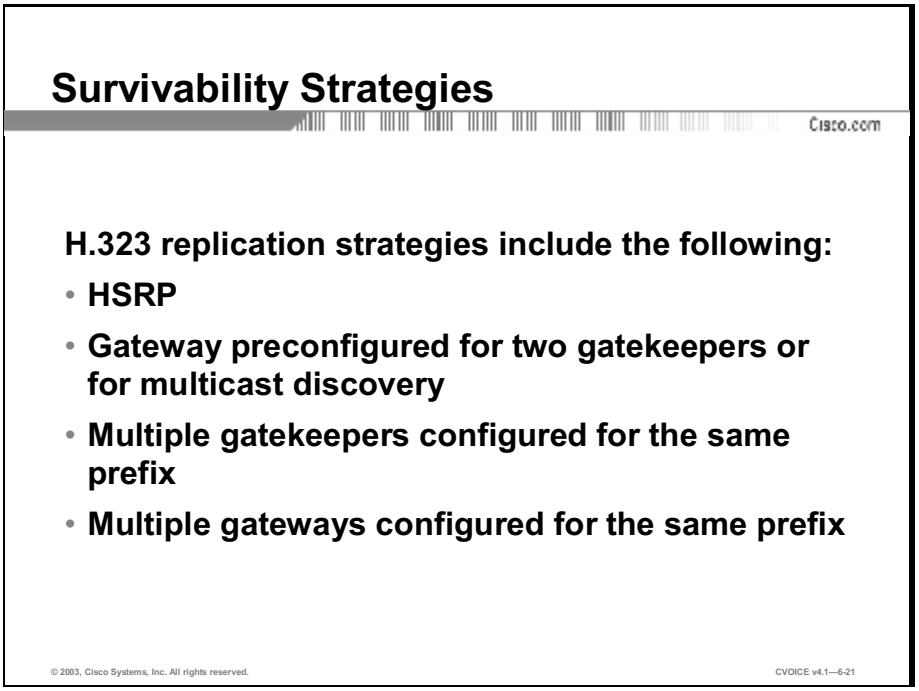


The figure illustrates a call setup involving two gatekeepers. In this example, each endpoint is registered with a different gatekeeper. Notice the changes in the call setup procedure.

1. The originating endpoint sends an admission request 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.

Survivability Strategies

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.



In any environment that depends on common control components, the vulnerability of the environment is directly proportional to the probability of 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 the following strategies:

- **Hot Standby Router Protocol:** The Hot Standby Router Protocol (HSRP) allows two gatekeepers to share both an IP address and access to a common LAN; however, at any time, only one is active. Endpoints are configured with the name of the gatekeeper, which they can resolve using Domain Name System (DNS), or the IP address of the gatekeeper.

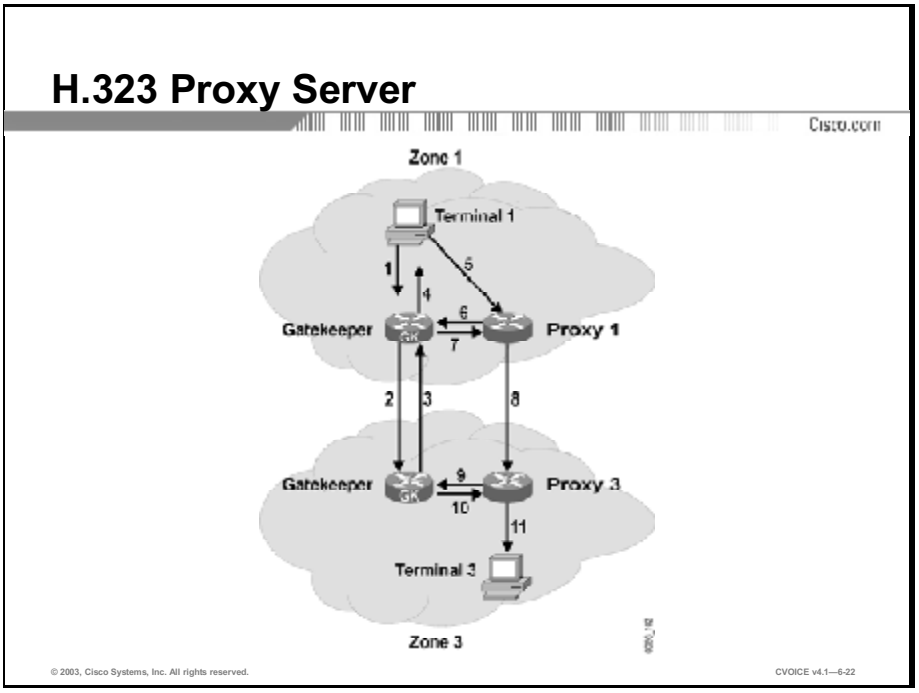
- **Multiple gatekeepers with gatekeeper discovery:** Deployment of multiple gatekeepers reduces the probability of total loss of gatekeeper access. However, adding new gatekeepers presents a new challenge. Each gatekeeper creates a unique H.323 zone. Because an H.323 endpoint is associated with only 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 messages to other gatekeepers when locating an endpoint. By supporting the same prefix on multiple gatekeepers, the location request 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 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, is not easily available because of a firewall, or zones are configured as inaccessible on the gatekeepers to isolate addressing information in different zones.

When a proxy server is involved, typically two sessions are 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

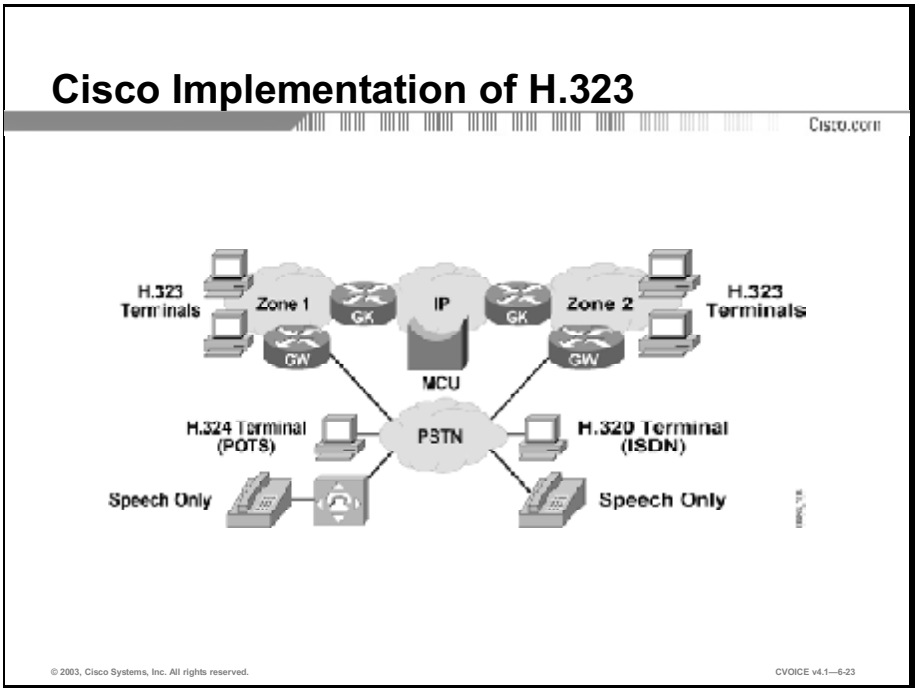
The figure illustrates an example with three sessions. The objective in this scenario is for terminal 1 and terminal 3 to establish an end-to-end relationship for multimedia communications. The following sequence of events occurs:

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.



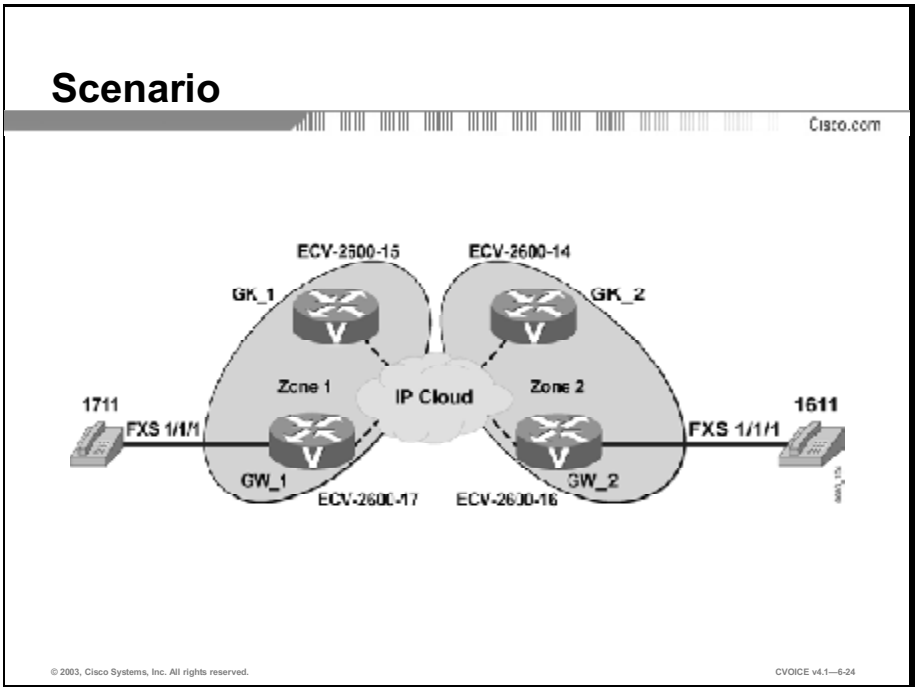
Cisco provides support for all H.323 components. These H.323 components include the following:

- **H.323 terminals:** Cisco provides support for H.323 terminals in Cisco IP Phone.
- **Gateways:** Cisco implements H.323 gateway support in:
  - Cisco voice-enabled routers (first available in Cisco IOS® release 11.3)
  - Cisco SC2200 signaling controllers
  - Cisco PGW 2200 PSTN Gateways
  - Voice-enabled AS5*xx*0 access servers
  - BTS 10200 Softswitch

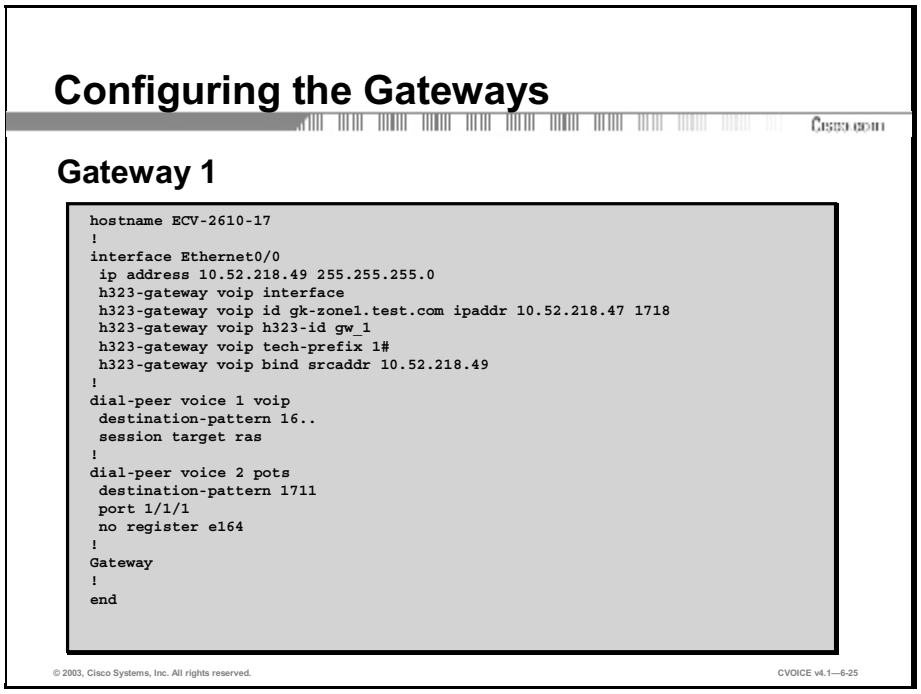
- **Gatekeepers:** Cisco implements gatekeeper support in:
  - Cisco Multimedia Conference Manager
  - Cisco CallManager
  - Routers (first available in Cisco IOS release 11.3)
- **Multipoint control unit:** The MC and MP of the Cisco IP/VC 3500-series MCU support all H.323 conference types. The IP/VC 3500 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 RTP sessions.

Configuring H.323 Gateways

This topic illustrates and describes the configuration commands used to create a two-zone, two-gatekeeper scenario.

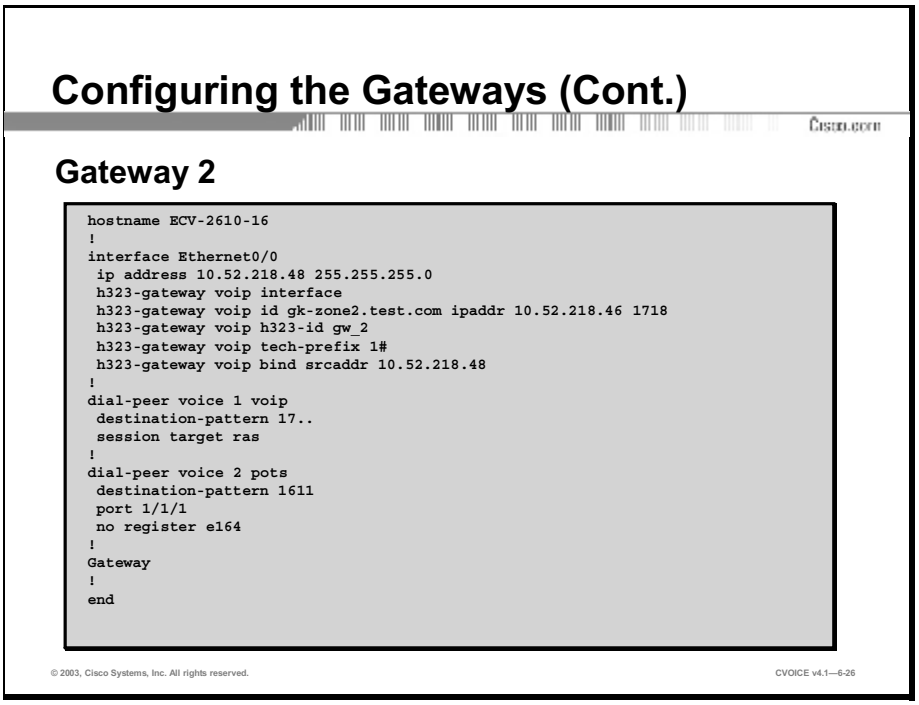


The figure illustrates the scenario on which the gateway configurations are based.



To use a gatekeeper, the user must complete the following three tasks on the gateway:

1. Enable the gateway with the **gateway** command.
2. Configure the relationship with the gatekeeper. This requires three interface subcommands:
   - **h323-gateway voip interface**: Tells the router that this interface should be enabled for H.323 packet processing
   - **h323-gateway voip id**: Identifies the ID of the gatekeeper
   - **h323-gateway voip h323-id**: 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** parameter on the dial peer subcommand **session target**.



You can use other interface subcommands, two of which are illustrated in the configuration for Gateway 2. These commands perform the following functions:

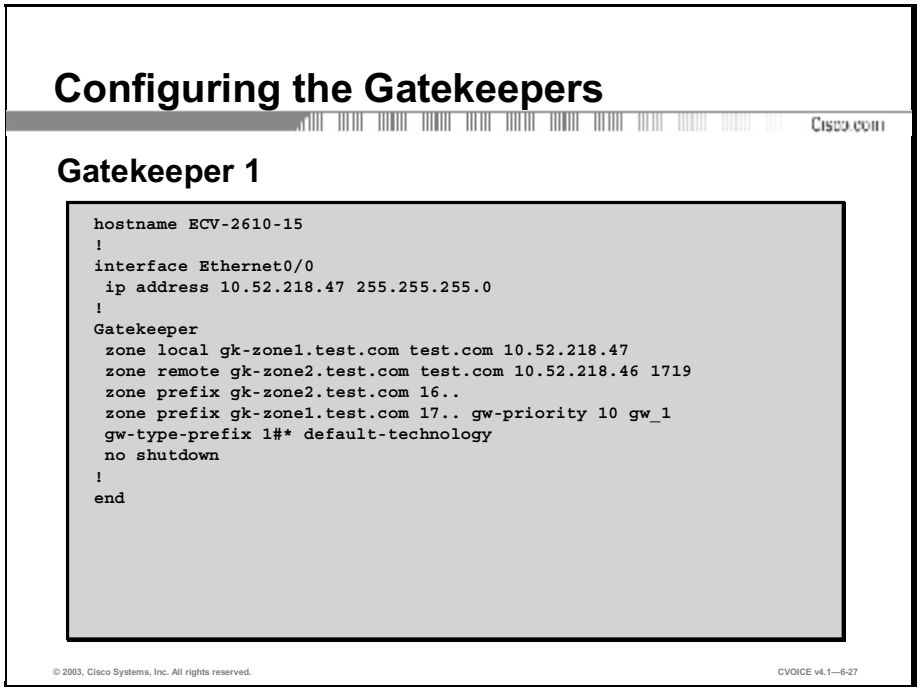
- **h323-gateway voip tech-prefix 1#:** Registers a technology prefix
- **h323-gateway voip bind srcaddr 10.52.218.48:** Sets the source address in H.323 packets

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.



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 the following 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.)

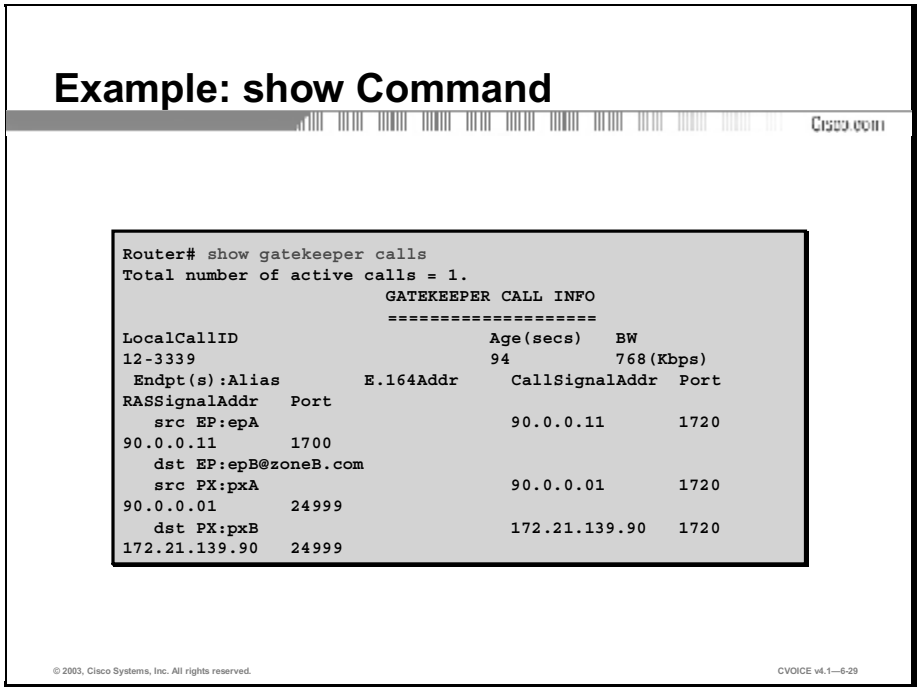
Gatekeeper 2

```
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.. gw-priority 10 gw_2
 zone prefix gk-zone1.test.com 17..
 gw-type-prefix 1#* default-technology
 no shutdown
!
end
```


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** 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.



Following 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:** Lists the registered endpoints with ID and supported prefixes
- **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

The **debug** commands used for H.323 include the following:

- **debug voip ccapi inout:** Shows every interaction with the call control 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 is highly active, use it sparingly in a live network.

- **debug cch323 h225:** 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:** 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:** Traces the state transition in the establishment of the 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:** Displays an expansion of the 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.

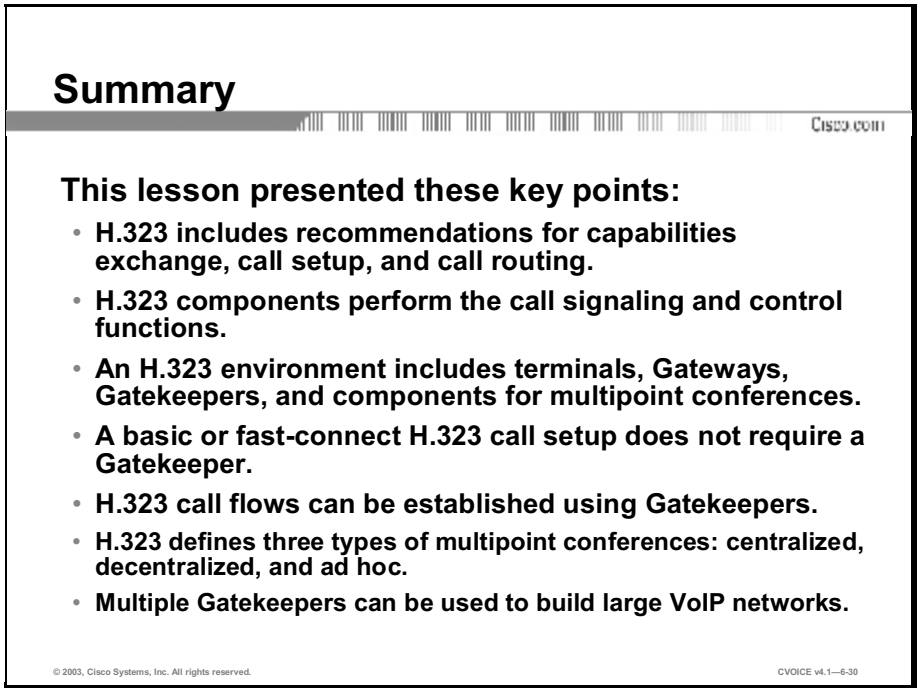
- **debug h225 events:** Similar to the ASN.1 version of the command but does not expand the ASN.1. Debugging events usually imposes a lighter load on the router.

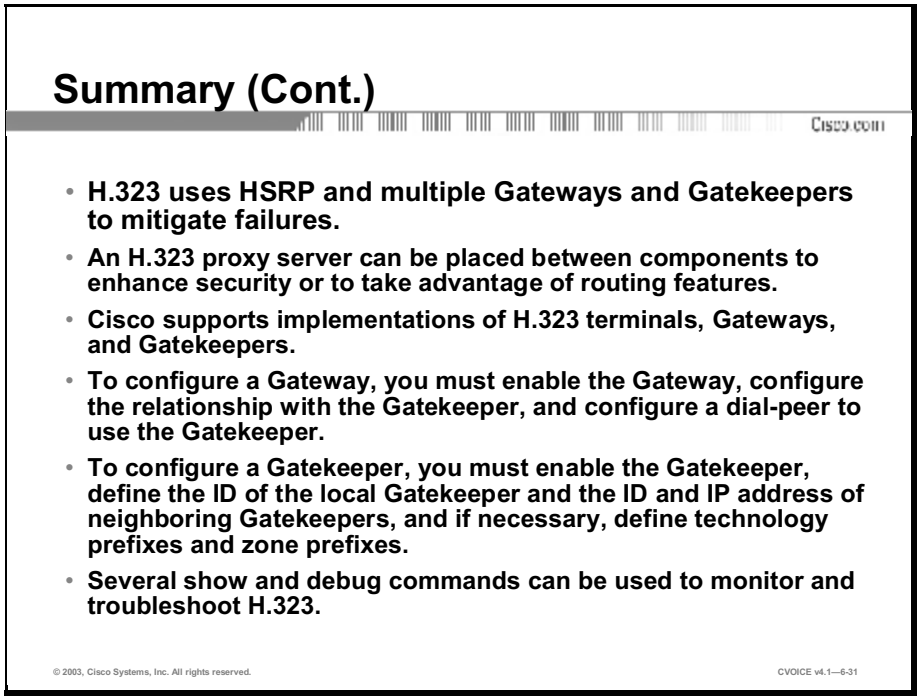
- **debug h245 asn1:** Similar to the H.225.0 variant except that it displays only the H.245 messages.

- **debug h245 events:** Similar to the H.225.0 variant except that it displays only the H.245 messages.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): H.323
- Assessment (Complex Lab): Refer to Lab 6-1, contained in Laboratory Exercises in Additional Resources section E.
- SIP lesson

References

For additional information, refer to these resources:

- “ITU-T Recommendation H.323”
- “Cisco IOS Voice, Video, and Fax Configuration Guide”
- “Cisco IOS Voice, Video, and Fax Command Reference”

Quiz: H.323

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the recommendations that are associated with H.323 and the control and signaling functions they perform
- List the functions that are performed by the components of 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
- Describe three types of multipoint conferences that are supported by H.323
- Provide a scenario of call flow with multiple gatekeepers and explain how this allows scalability
- Describe four strategies that are used by H.323 to provide fault tolerance networks
- List the steps involved in using an H.323 proxy server to set up end-to-end connections
- List the components that are supported by the Cisco Systems implementation of H.323
- Use the commands that are required to configure gateways in a two-zone, two-gatekeeper scenario
- Use the commands that are required to configure gatekeepers in a two-zone, two-gatekeeper scenario
- List the **show** and **debug** commands that are used to monitor and troubleshoot Cisco H.323 gateways and gatekeepers

Instructions

Answer these questions:

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

F) none of the above

Q7) Put in the correct order the steps involved in H.323 basic call setup without a gatekeeper.

_____ 1. Call setup procedures based on Q.931 create a call signaling channel between the endpoints.

_____ 2. The H.245 control function negotiates capabilities and exchanges logical channel descriptions.

_____ 3. The gateway determines the IP address of the destination gateway internally.

_____ 4. The logical channel descriptions open RTP sessions.

_____ 5. The endpoints open another channel for the H.245 control function.

_____ 6. The originating gateway initiates an H.225.0 session with the destination gateway on registered TCP port 1720.

_____ 7. The endpoints exchange multimedia over the RTP sessions.

Q8) How does the abbreviated call-setup procedure in version 2 of 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) It establishes an H.245 control channel with both endpoints.

B) It performs call setup, call function, and call control functions.

C) It represents the other endpoint for call signaling only.

D) It passes on the originating endpoint's request 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 admission request from the originating endpoint

C) the call setup request from the gateway

D) network statistics

Q11) 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

Q12) 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

Q13) 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

Q14) In a call flow with multiple gatekeepers, which gatekeeper allows the remote endpoint to accept the incoming call?

A) the gatekeeper that the originating endpoint is associated with

B) the gatekeeper that the remote endpoint is associated with

C) the gatekeeper that first received the admission request

D) the gatekeeper that is available to set up the call

Q15) In H.323, which survivability strategy allows two gatekeepers to share an IP address?

A) HSRP

B) multiple gateways configured for the same prefix

C) multiple gatekeepers configured for the same prefix

D) multiple gatekeepers with gatekeeper discovery

Q16) 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.

Q17) What is the role of an H.323 proxy server?

A) provides an alternate path when the direct path is not the most appropriate path

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

Q18) 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

Q19) Which Cisco application supports H.323 gatekeepers?

A) Cisco IP Phone

B) Cisco CallManager

C) Cisco Secure Integrated Software

D) Cisco voice-enabled switches

Q20) Which H.323 component is supported by Cisco SC2200 signaling controllers?

A) terminals

B) gateways

C) gatekeepers

D) MCU

Q21) 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

Q22) When you are configuring an H.323 gateway, what 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

Q23) Which command tells the gatekeepers to define addresses locally?

A) **zone prefix**

B) **zone local**

C) **zone remote**

D) **zone default**

Q24) 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

Q25) Which **show** command is used to list the registered endpoints with ID and supported prefixes?

A) **show gatekeeper gw-type-prefix**

B) **show gatekeeper zone prefix**

C) **show gatekeeper endpoints**

D) **show gatekeeper status**

Q26) 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**

E) **none of the above**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

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.

Importance

An understanding of the features and functions of SIP components, and the relationships 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:

- Describe three Internet Engineering Task Force 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 Systems

- 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 fully benefit 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 Voice over IP (VoIP)

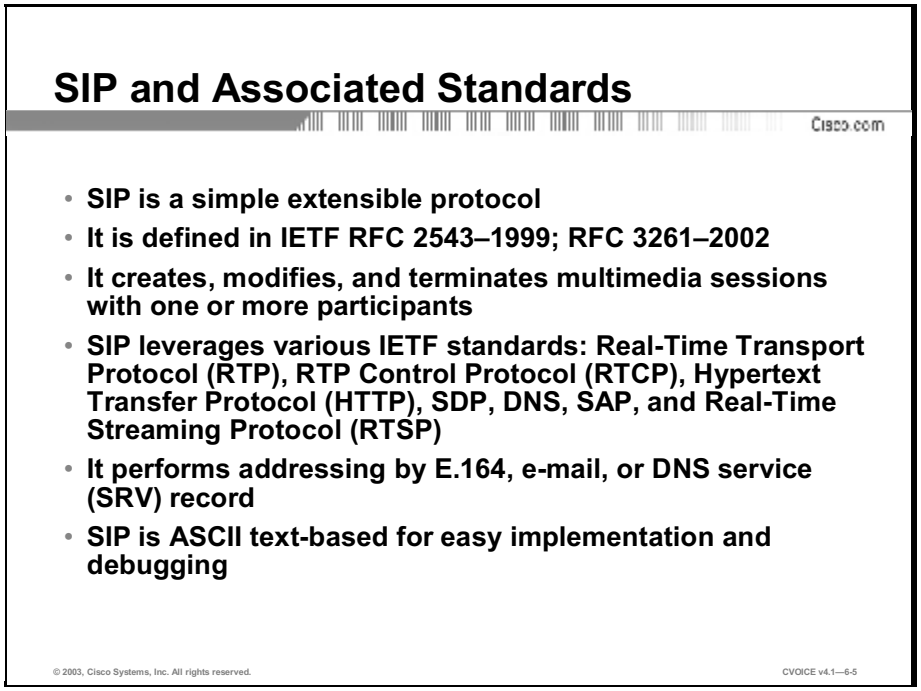
Outline

This lesson includes these topics:

- Overview
- SIP and Its Associated Standards
- Components of SIP
- SIP Messages
- SIP Addressing
- Call Setup Models
- Survivability Strategies
- Cisco Implementation of SIP
- Configuring SIP on a Cisco Router
- Monitoring and Troubleshooting
- Summary
- Assessment (Quiz): SIP
- Assessment (Complex Lab): Lab Exercise 6-2

SIP and Its Associated Standards

The session initiation protocol (SIP) provides another framework for establishing and maintaining Voice over IP (VoIP) calls. This topic describes SIP and its standards.



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 Definition 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, 800 services, and local number portability are just three of these services.

Multimedia sessions are established and terminated by the following services:

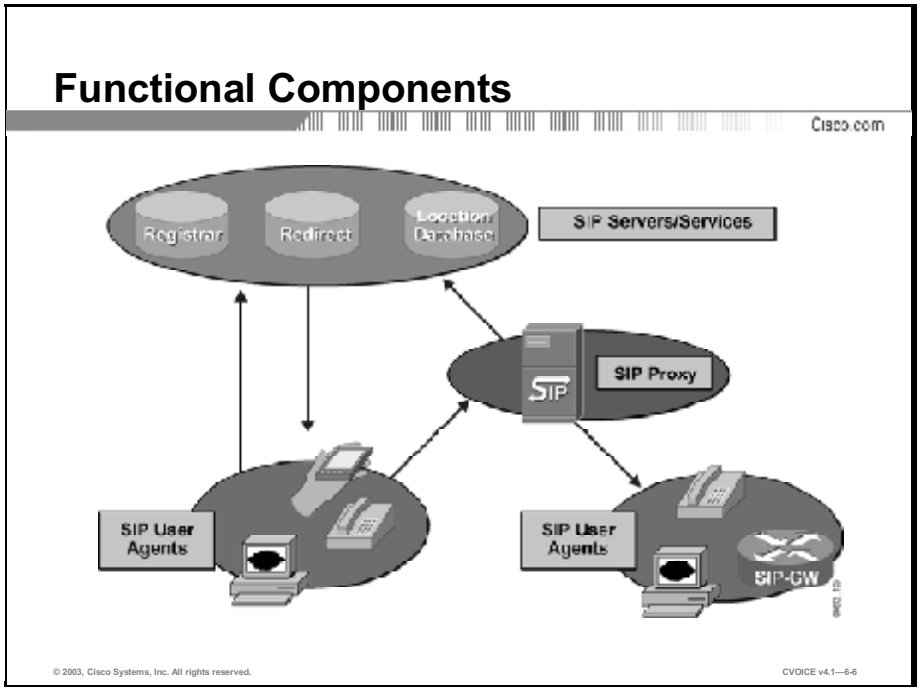
- **User location services:** Locate an end system
- **User capabilities services:** Select the media type and parameters
- **User availability services:** Determine the availability and desire for a party to participate
- **Call setup services:** Establish a session relationship between parties and 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).

Components of SIP

SIP is modeled on the interworking of user agents (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 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 the following two categories:

- **User agents:** SIP user agents include the following devices:
  - **IP telephone:** Acts as a UAS or UAC on a session-by-session basis. Software phones and Cisco Systems SIP IP Phones initiate SIP requests and respond to requests.

- **Gateway:** Acts as a UAS or UAC and provides call control support. Gateways provide many services, the most common being a translation function between SIP user agents and other terminal types. This function includes translation between transmission formats and between communications procedures. A gateway translates between audio and video signals and performs call setup and clearing on both the IP side and the switched circuit network (SCN) side.

- **SIP servers:** SIP servers include the following types:

  - **Proxy server:** Intermediate component that receives SIP requests from a client, then forwards the requests on behalf of the client to the next SIP server in the network. The next server can be another proxy server or a UAS. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request transmissions, and security.

  - **Redirect server:** Provides a 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.

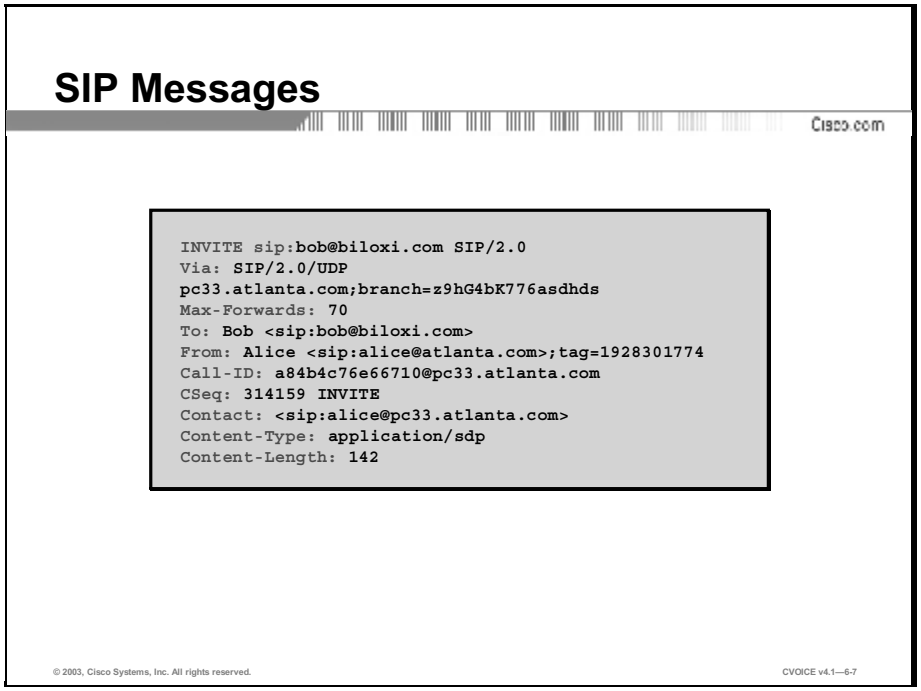
  - **Registrar server:** Requests from UACs for registration of their current location. Registrar servers are often located near or even colocated with other network servers, most often a location server.

  - **Location server:** An abstraction of a service providing address resolution services to SIP proxy or redirect servers. A location server embodies mechanisms to resolve addresses. These mechanisms can include a database of registrations or access to commonly used resolution tools such as finger, **rwhois**, Lightweight Directory Access Protocol (LDAP), or operating system-dependent mechanisms. A registrar server can be modeled as one subcomponent of a location server; the registrar server is partly responsible for populating a database associated with the location server.

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

SIP Messages

Communication between SIP components uses a request and/or response message model. This topic describes the types, use, and structure of these messages.

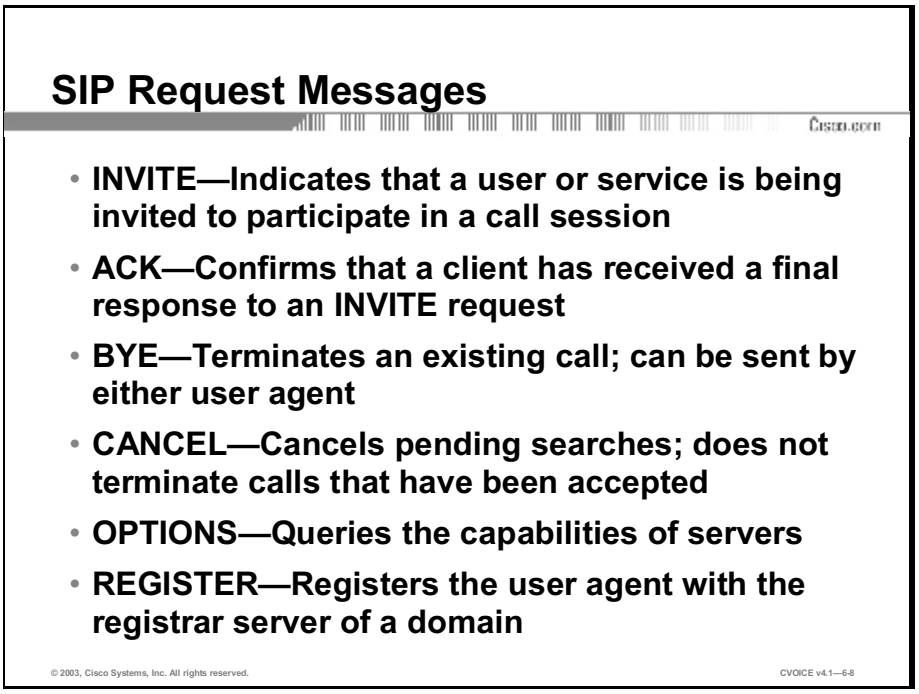


SIP communication involves two messages:

- **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 ARPA Internet Text Messages*, and RFC 2068, *Hypertext Transfer Protocol — HTTP/1.1*.

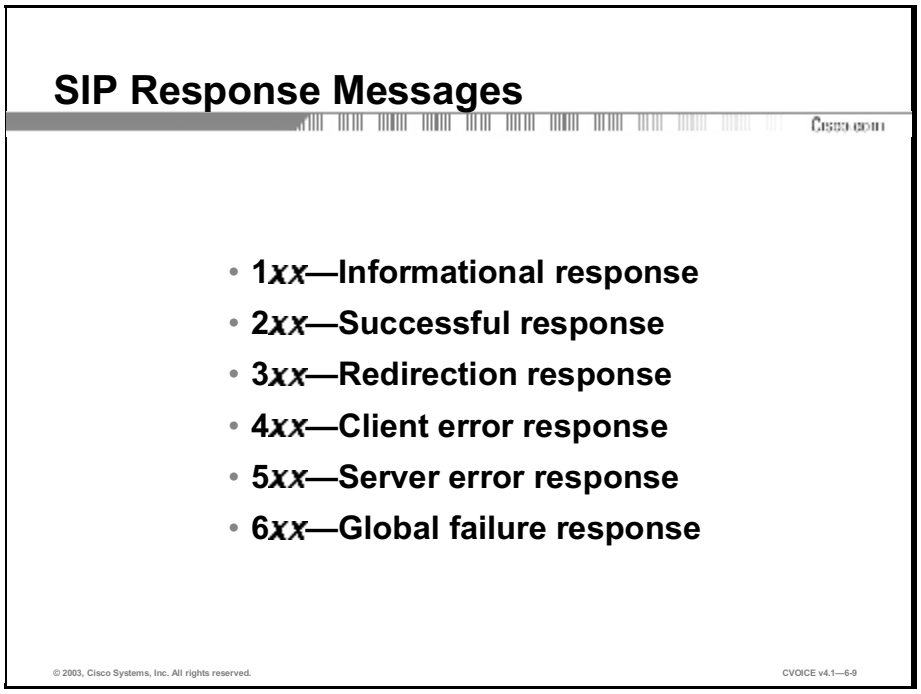
SIP defines 4 types of headers: a general header, an entity header, a request header, and a response header. The first two appear on both message types. The latter two are specific to request and response respectively.



In the request line, SIP uses a "method" to indicate the action to be taken by the responding component (usually a server).

The following request methods indicate the action that the responding component should take:

- **INVITE:** A client originates the INVITE method to indicate that the server is invited to participate in a session. An invitation includes a description of the session parameters.
- **ACK:** A client originates the ACK method to indicate that the client has received a response to its earlier invitation.
- **BYE:** A client or server originates the BYE method to initiate call termination.
- **CANCEL:** A client or server originates the CANCEL method to interrupt any request currently in progress. CANCEL is *not* used to terminate active sessions.
- **OPTIONS:** A client uses the OPTIONS method 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 accept an incoming call.
- **REGISTER:** A UA uses the REGISTER method 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 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.

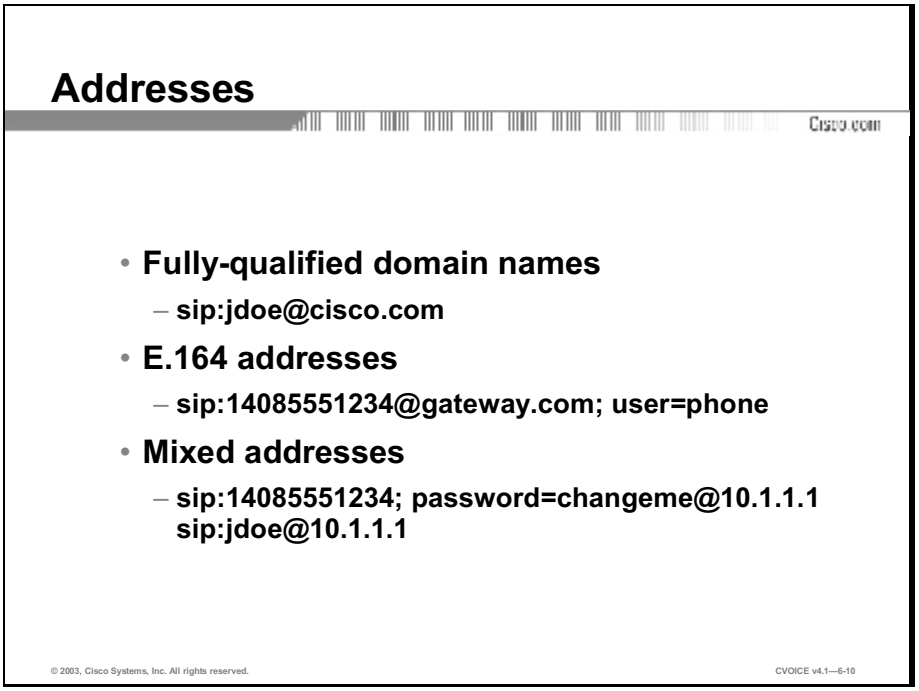
Status Codes

The following response messages indicate the status of a request:

- **1xx—Informational:** (Provisional response) Indicates that the request is still being processed.
- **2xx—Success:** 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.



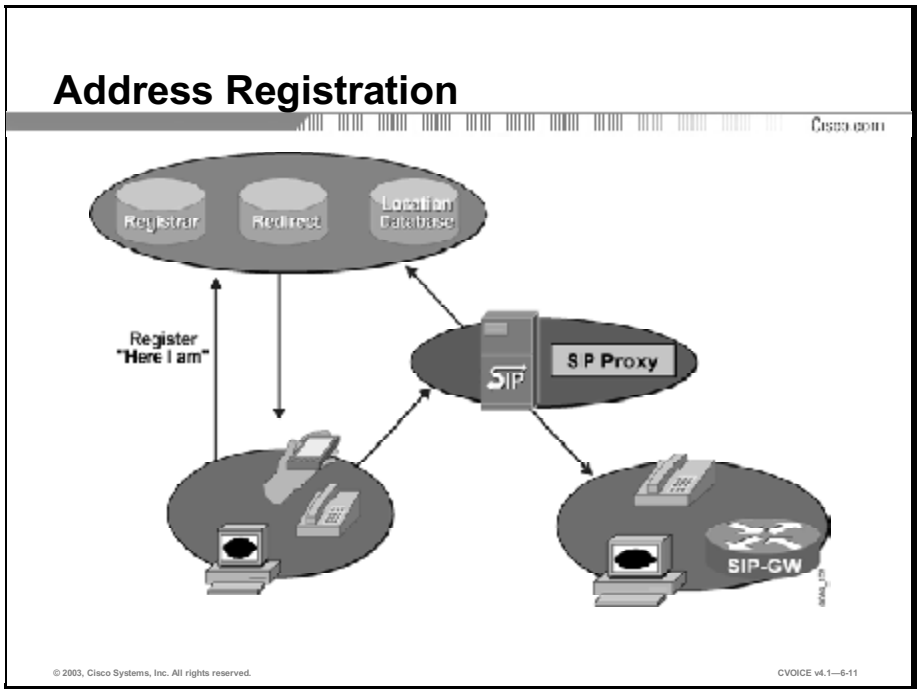
An address in SIP is defined in the syntax for a URL with sip: or sips: (for secure SIP connections) as the URL type. SIP URLs are used in SIP messages to identify the originator, the current destination, the final recipient, and any contact party. When two UAs communicate directly with each other, the 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 with the host description.

Example

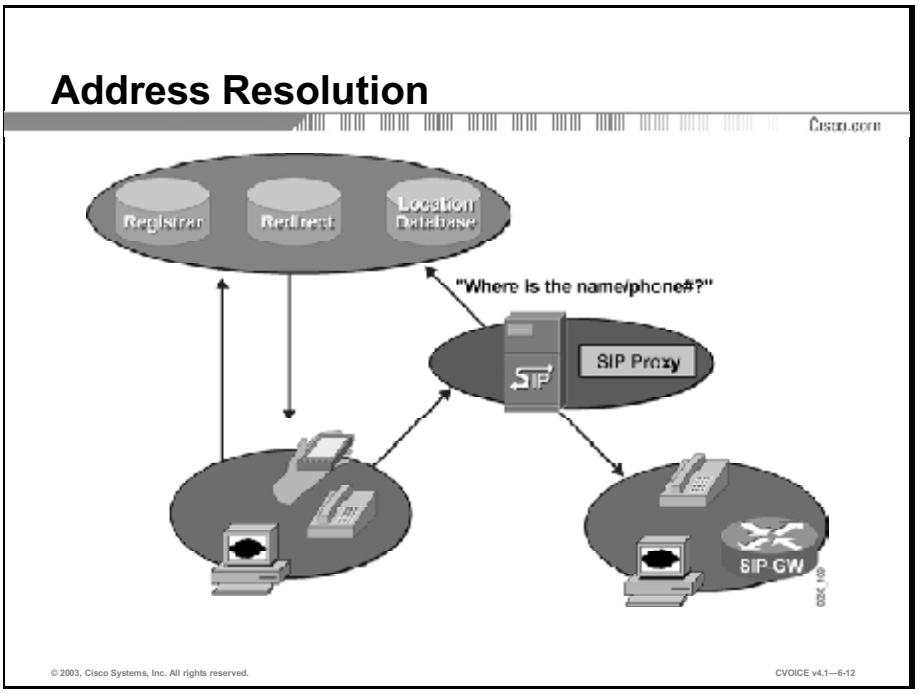
The figure provides examples of SIP addresses.

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 **14085559876** in the URL **sip:14085559876@10.1.1.1** is an example of a numeric user ID. In the same example, the password **changeme** is defined for the user.



A SIP address is acquired in several ways. For example, an address is acquired 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 REGISTER mode request to a registrar server.

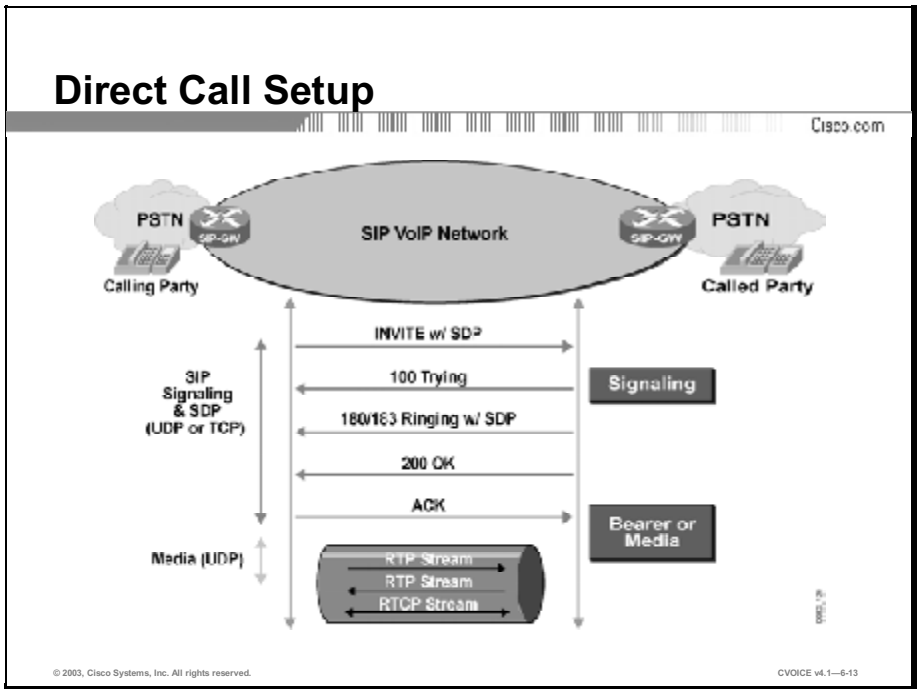


To resolve an address, aA UA uses a variety of internal mechanisms such as a local host table, DNS lookup, finger, **rwhois**, or LDAP, or it leaves that responsibility to a network server. A network server uses any of the tools available to a UA or interacts through a nonstandard interface with a location 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 where 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.



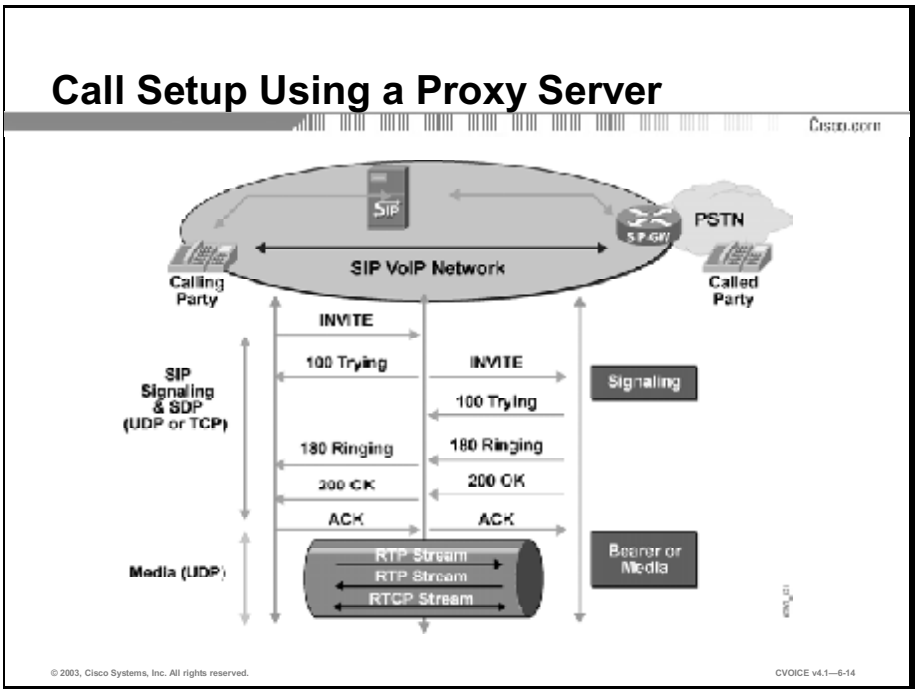
When a UA recognizes the address of a terminating endpoint from cached information, or has the capacity to resolve it by some internal mechanism, the UAC may initiate direct (UAC-to-UAS) call setup procedures.

Direct setup is the fastest and most efficient of the call setup procedures. However, it does have 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 nonscalable.

Direct call setup proceeds as follows:

1. The originating UAC sends an invitation (INVITE) to the UAS of the recipient. The message includes an end-point 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 RTP sessions between them.



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.

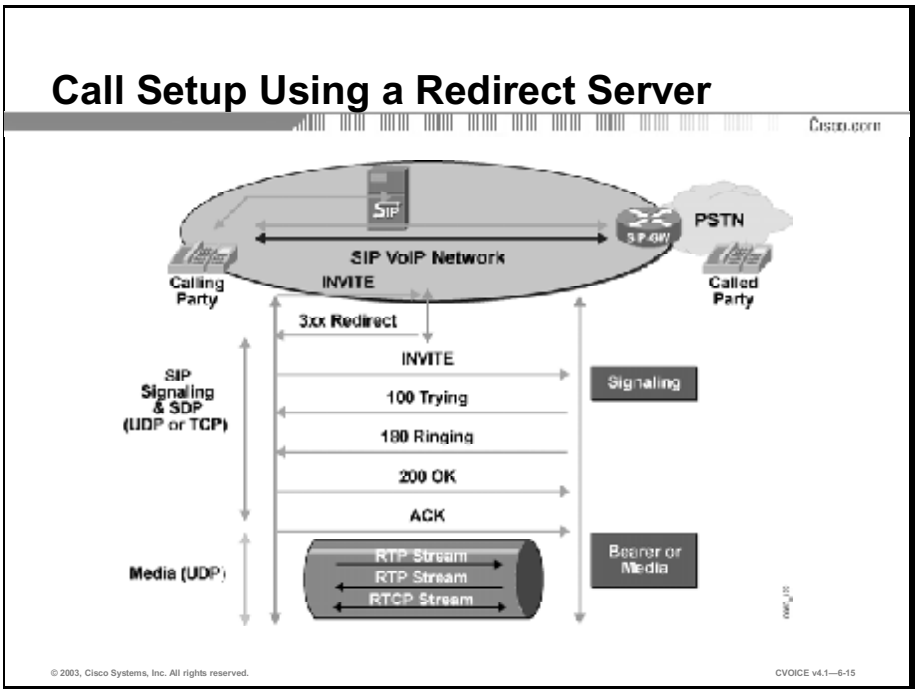
Note	Although the proxy server acts on behalf of a UA for call setup, the UAs establish RTP sessions directly with each other.

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 invitation 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.



A redirect server is programmed to discover a path to the destination; instead of forwarding the invitation 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.

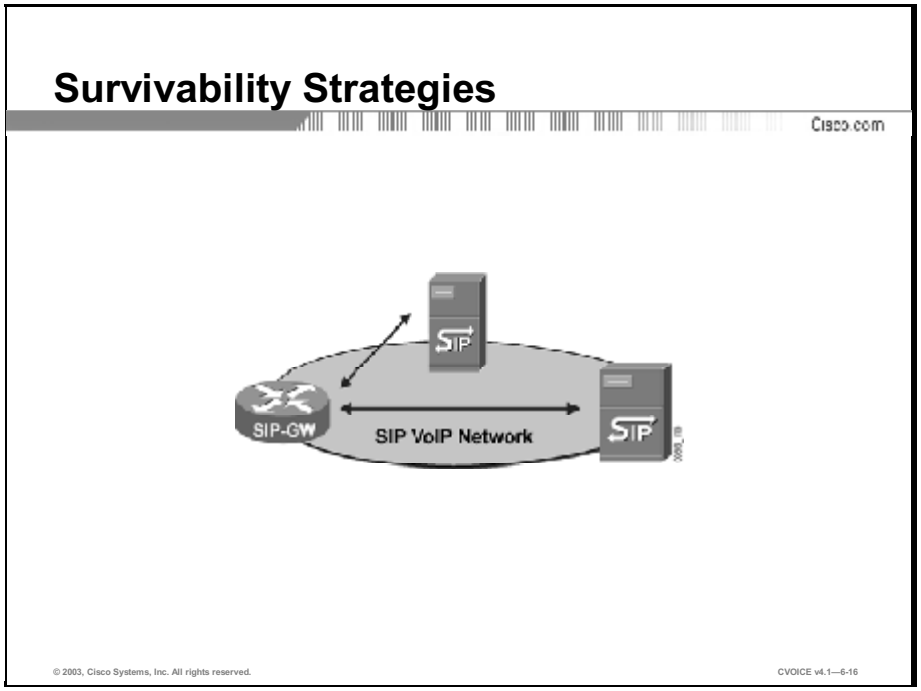
When a redirect server is used, the call setup procedure is as follows:

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 invitation 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 acknowledgment.

The UAC and UAS now have all the information required to establish RTP sessions between them.

Survivability Strategies

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.

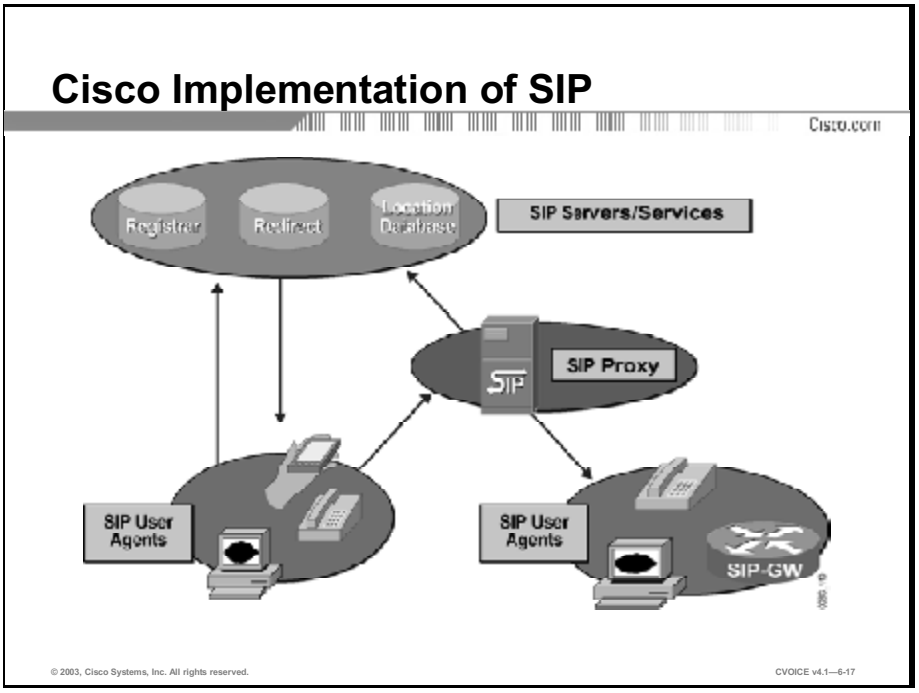
For replication of a proxy or redirect server to be effective, a UA must have the ability to locate an active server dynamically. You can achieve this in any of the following ways:

- 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.

Cisco Implementation of SIP

This topic describes how Cisco implements SIP.



Cisco provides support for the following SIP components:

- **SIP user agents:** Cisco provides support for SIP UA in Cisco IP Phone.

  Cisco implements SIP UA (gateway) support in the following devices:

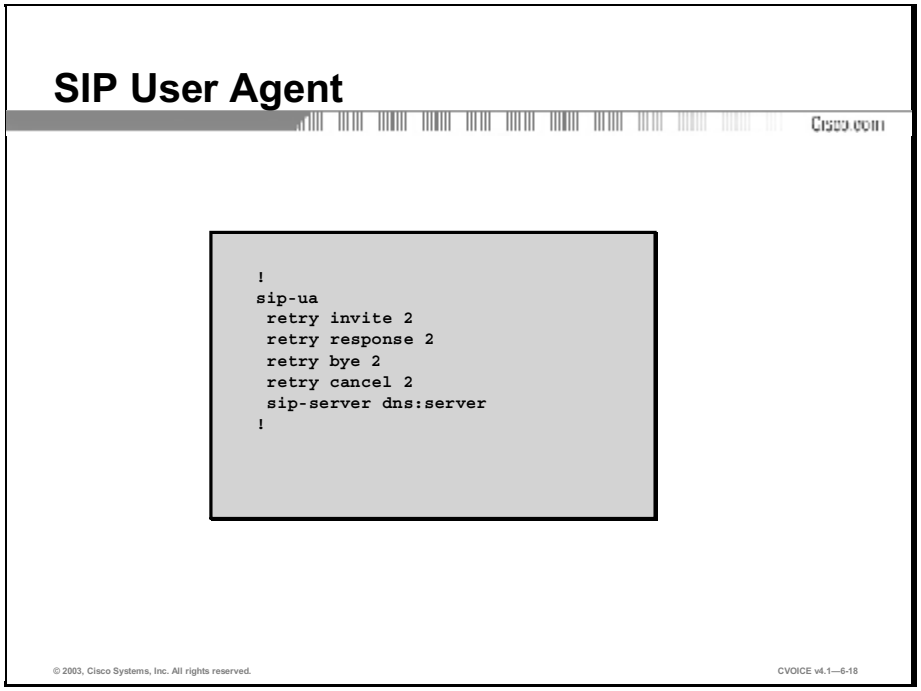
  - Cisco voice-enabled routers (first available in Cisco IOS® release 12.1)
  - Cisco PGW 2200 PSTN gateways
  - Voice-enabled AS5*xx*0 access servers
  - BTS 10200 Softswitch

- **Network servers:** Cisco implements SIP proxy and redirect server support in the Cisco SIP proxy server. The server is an application designed for a Linux (Redhat 7.1) or Solaris 2.8 operating environment

- **Other support:** Cisco PIX 500 series firewalls monitor the SIP handshaking to dynamically open conduits for the RTP sessions.

Configuring SIP on a Cisco Router

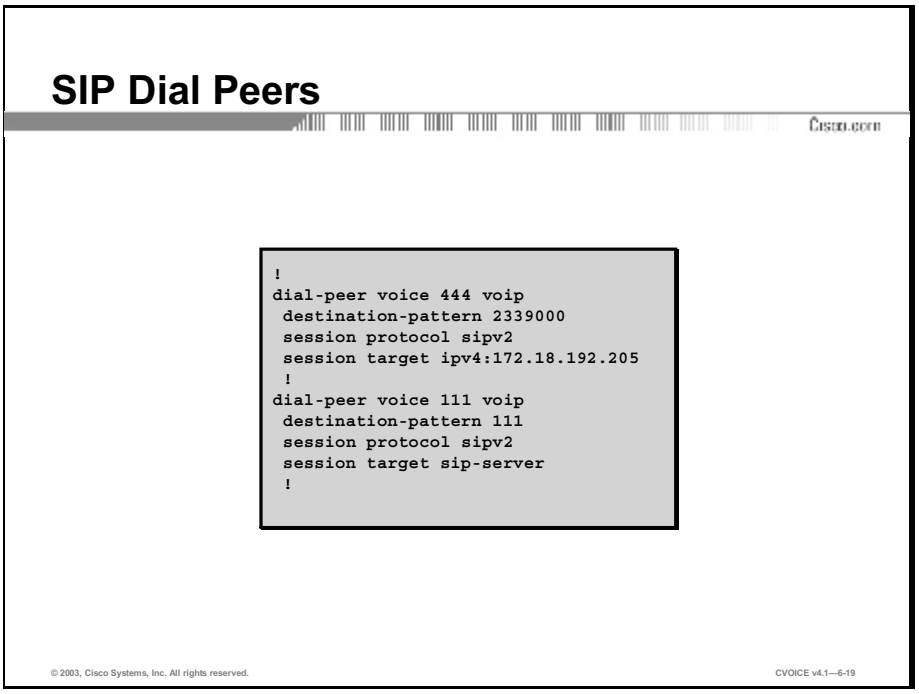
A SIP configuration consists of two parts: the SIP UA and the VoIP dial peers that select SIP as the session protocol. This topic illustrates and describes the configuration commands that you must use to implement SIP call setup models.



The SIP UA is one part of the SIP configuration. The figure shows an example of a SIP UA configuration.

Example

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 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

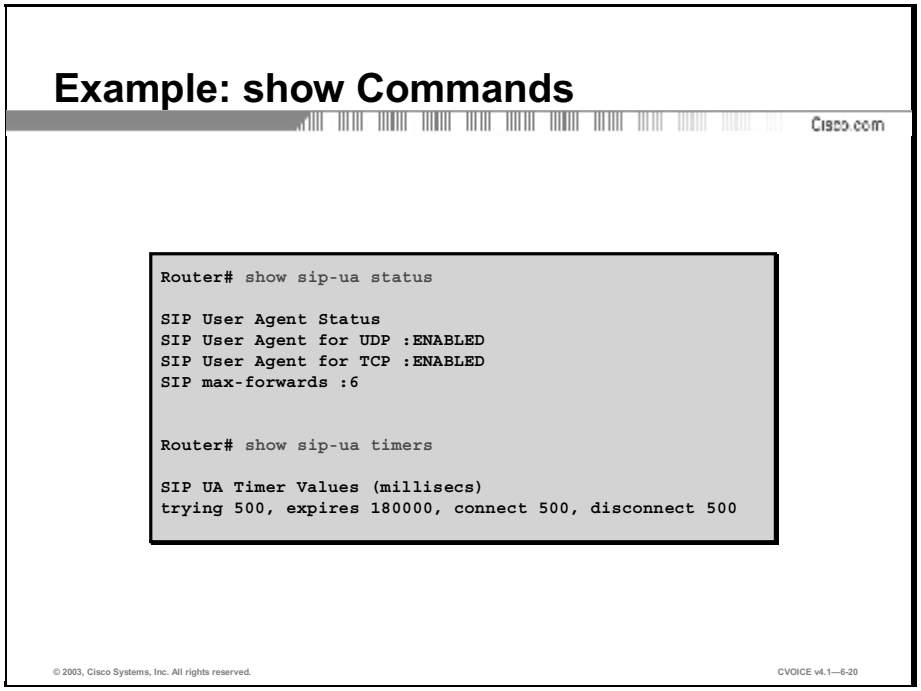
In the example, both dial peers include **session protocol sipv2 and** SIP is used when the destination pattern matches either dial peer. The session target distinguishes one session from the other.

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 **sip-server**. When **sip-server** is the target, the IP address of the actual server is taken from the **sip-server** subcommand in the SIP UA configuration. 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.



The following **show** commands 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 following **debug** commands are valuable when examining the status of SIP components and troubleshooting:

- **debug voip ccapi inout:** Shows every interaction with the call control application program 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 is very active; you must use it sparingly in a live network.

- **debug ccsip all:** Enables all **ccsip** type debugging. This debug is very active; you must use it sparingly in a live network.

- **debug ccsip calls:** Displays all SIP call details as they are updated in the SIP call control block. You must use this debug to monitor call records for suspicious clearing causes.

- **debug ccsip errors:** Traces all errors encountered by the SIP subsystem.

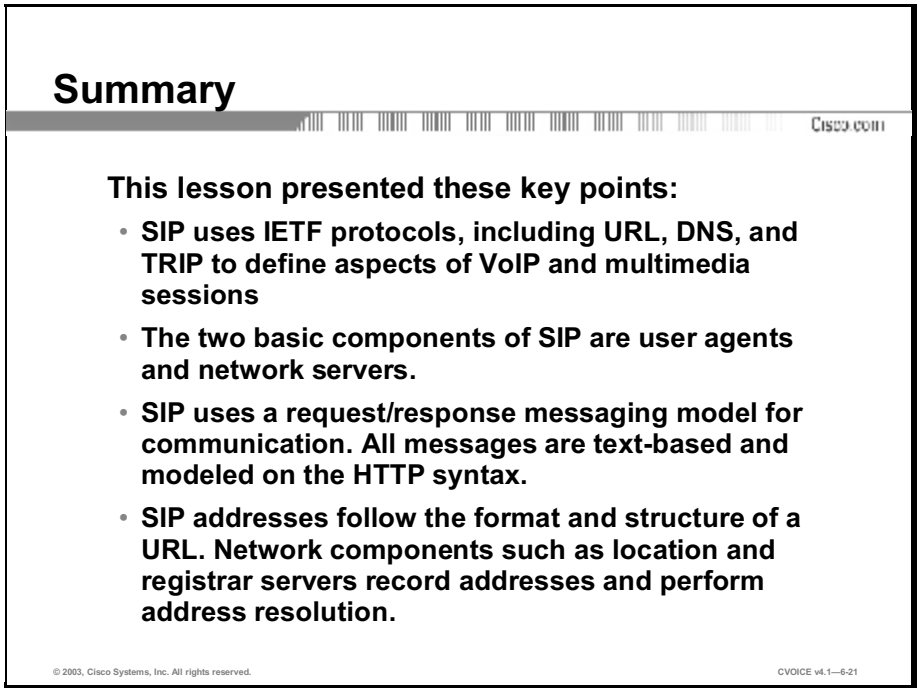
- **debug ccsip events:** Traces events, such as call setups, connections, and disconnections. An **events** version of a debug is often the best place to start, as detailed debugs provide a great deal of useful information.

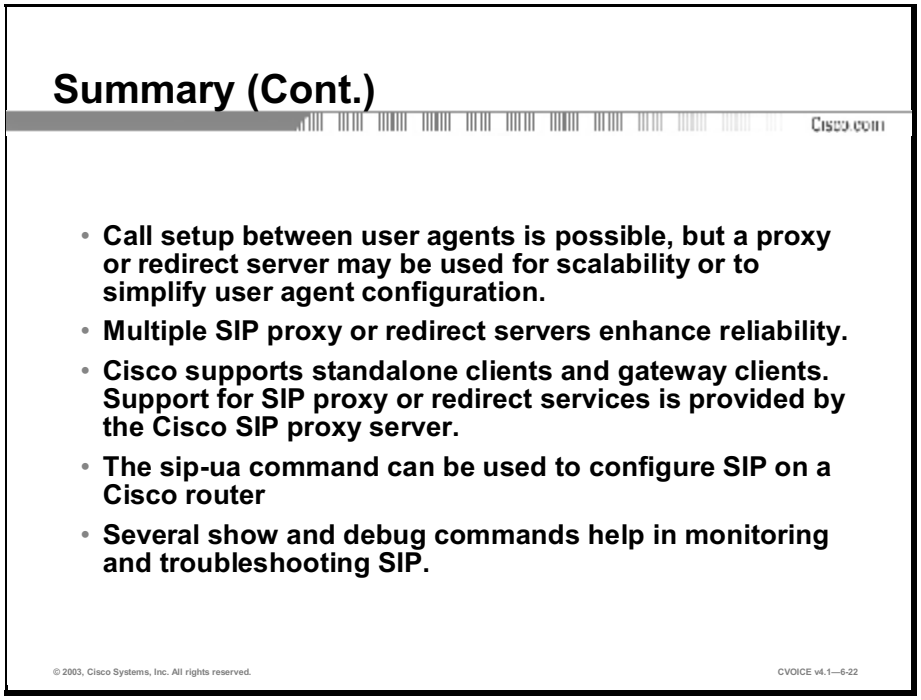
- **debug ccsip messages:** Shows the headers of SIP messages that are exchanged between a client and a server.

- **debug ccsip states:** Displays the SIP states and state changes for sessions within the SIP subsystem.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): SIP
- Assessment (Complex Lab): Refer to Lab 6-2, contained in Laboratory Exercises in Additional Resources section E.
- MGCP lesson

References

For additional information, refer to these resources:

- “IETF RFC 3261, SIP: Session Initiation Protocol”
- “Cisco IOS Voice, Video, and Fax Configuration Guide”
- “Cisco IOS Voice, Video, and Fax Command Reference”

Quiz: SIP

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe three Internet Engineering Task Force 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 Systems
- Use the **sip-ua** command with subcommands to configure SIP on a Cisco router
- Use **show** and **debug** commands to monitor and troubleshoot SIP

Instructions

Answer these questions:

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) Which of the following is NOT a SIP server?

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 method 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) 1*xx*—Informational

B) 2*xx*—Successful

C) 3*xx*—Redirection

D) 4*xx*—Client error

E) 5*xx*—Server error

F) 6*xx*—Global failure

Q7) How does a SIP UA resolve an address?

A) It uses a local host table.

B) It uses **rwhois.**

C) It lets the network server resolve it.

D) All of the above.

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) Which SIP component is supported by Cisco voice-enabled AS5*xx*0 servers?

A) SIP user agent

B) SIP proxy server

C) SIP redirect server

D) SIP dial peer

Q14) Which operating environments can Cisco SIP proxy server be used with?

A) Linux (Redhat 8.0 or later)

B) Windows NT

C) Solaris 2.8

D) MacOS

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**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

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 the features and functions of the MGCP environment.

Importance

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:

- Define MGCP and its functions
- List the basic components of MGCP
- Name eight types of MGCP endpoints defined in RFC 2705 and identify their functions
- Name seven types of MGCP gateways defined in RFC 2705 and identify their functions
- Describe the function of a call agent in an MGCP environment
- List the basic concepts of MGCP
- List the steps involved in the process of MGCP call establishment
- Describe the function of MGCP events and signals and give five examples of each

- List eight types of MGCP gateways and the packages that are associated with each gateway
- Explain how digit maps reduce the load on the network during call setup
- List nine MGCP control messages that are used to control and manage endpoints and their connections
- Describe MGCP call setup and control procedures
- Identify two strategies implemented by Cisco Systems to provide high availability in an MGCP environment
- Identify the Cisco devices that implement MGCP
- Use the **mgcp** command and subcommands to configure an MGCP residential and trunk gateway on a Cisco router
- Use **show** and **debug** commands to monitor and troubleshoot MGCP

Learner Skills and Knowledge

To fully benefit 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 Voice over IP (VoIP)

Outline

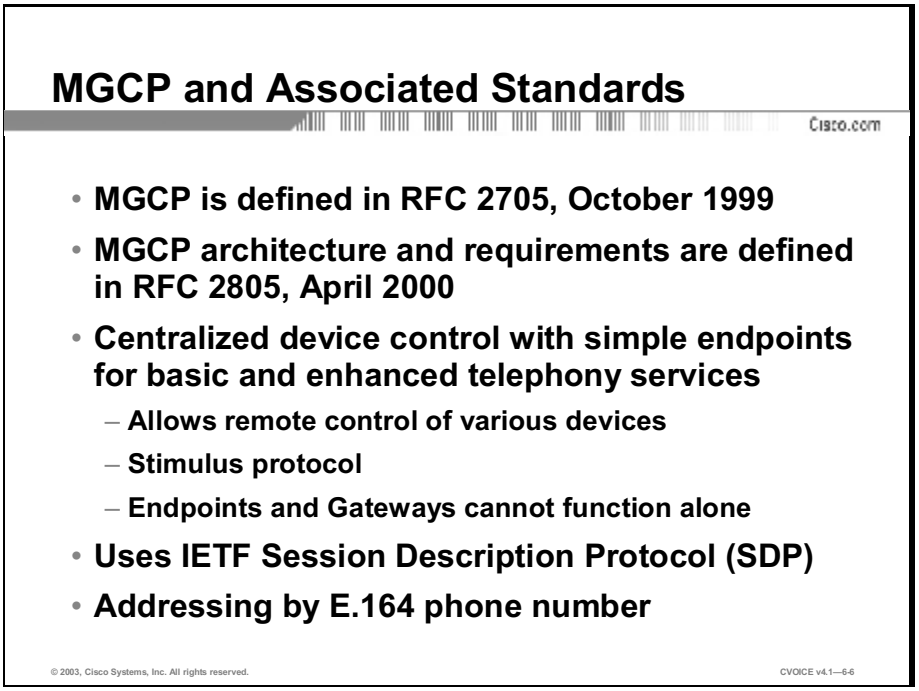
This lesson includes these topics:

- Overview
- MGCP and Its Associated Standards
- Basic MGCP Components
- MGCP Endpoints
- MGCP Gateways
- MGCP Call Agents
- Basic MGCP Concepts
- MGCP Calls and Connections
- MGCP Events and Signals

- MGCP Packages
- MGCP Digit Maps
- MGCP Control Commands
- Call Flows
- Survivability Strategies
- Cisco Implementation of MGCP
- Configuring MGCP
- Monitoring and Troubleshooting MGCP
- Summary
- Assessment (Quiz): MGCP
- Assessment (Complex Lab): Lab Exercise 6-3

MGCP and Its Associated Standards

Media Gateway Control Protocol (MGCP) controls telephony gateways from a centralized call agent. This topic describes MGCP and identifies its associated standards.

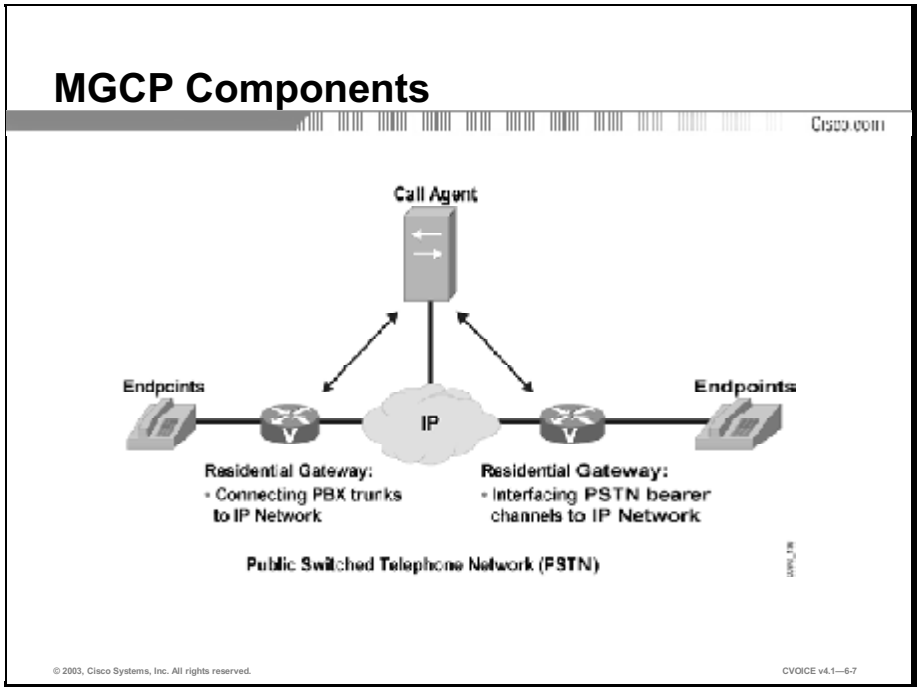


MGCP defines an environment for controlling telephony gateways from a centralized call control component known as a call agent. An MGCP gateway handles the translation of audio between the telephone switched-circuit network (SCN) and the packet switched network of the Internet. Gateways interact with a call agent that performs signaling and call processing.

The 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.



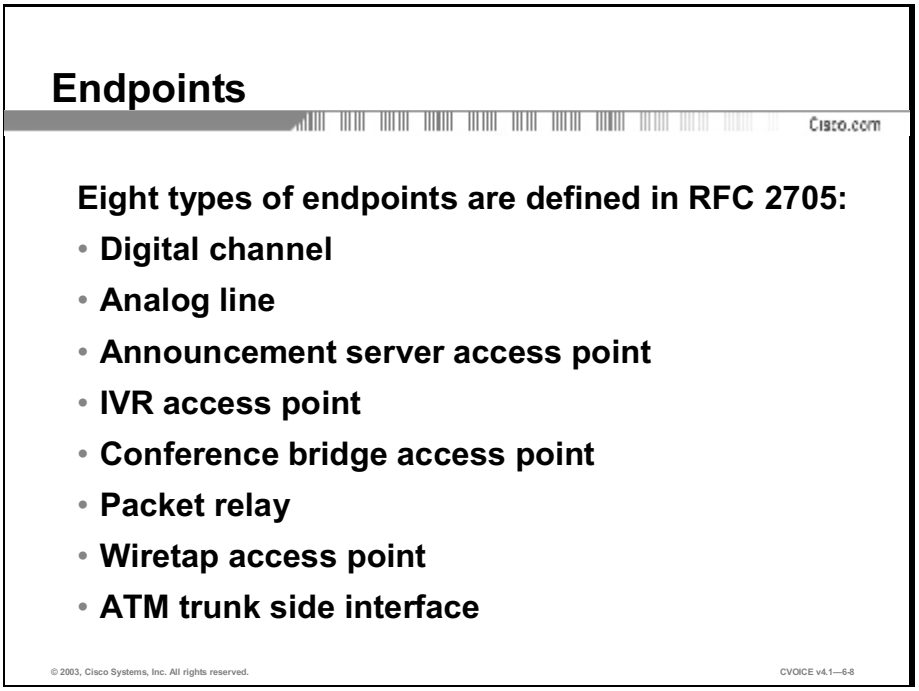
The following components are used in an MGCP environment:

- **Endpoints:** Represents the point of interconnection between the packet network and the traditional telephone network
- **Gateways:** Handles 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.

MGCP Endpoints

This topic lists the standard endpoints and defines the way that identifiers are associated with an endpoint.



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 zero (DS0):** Represents a single channel (DS0) in the digital hierarchy. A digital channel endpoint supports more than one connection.

- **Analog line:** 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:** 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.

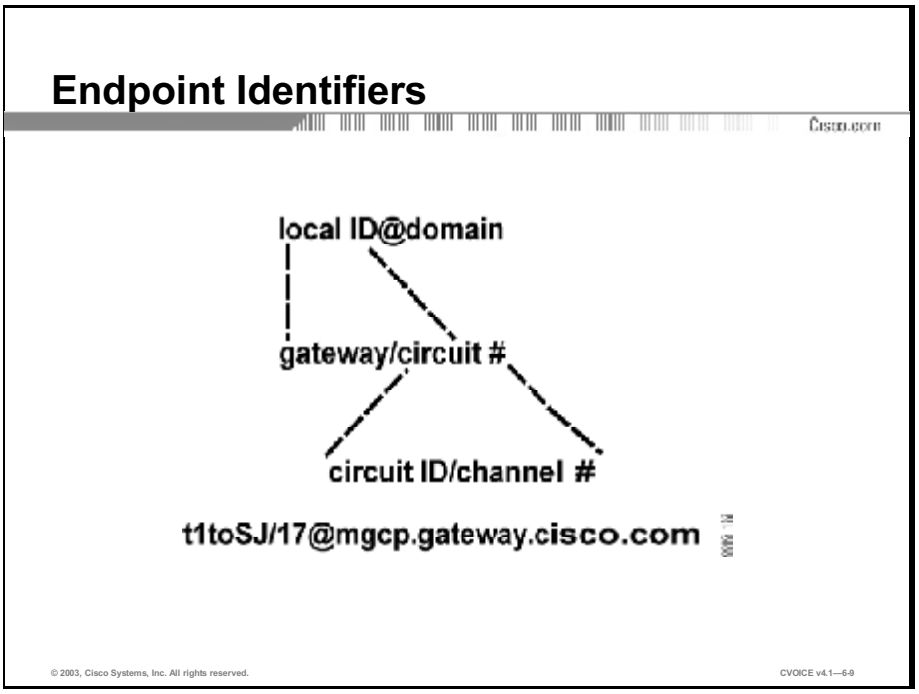
- **Interactive voice response (IVR) access point:** Represents access to an IVR service. An IVR endpoint has one connection. Multiple users of the IVR system are modeled to use different endpoints.

- **Conference bridge access point:** 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:** 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:** Represents access for recording or playing back a connection. A wiretap access point endpoint has one connection.

- **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.

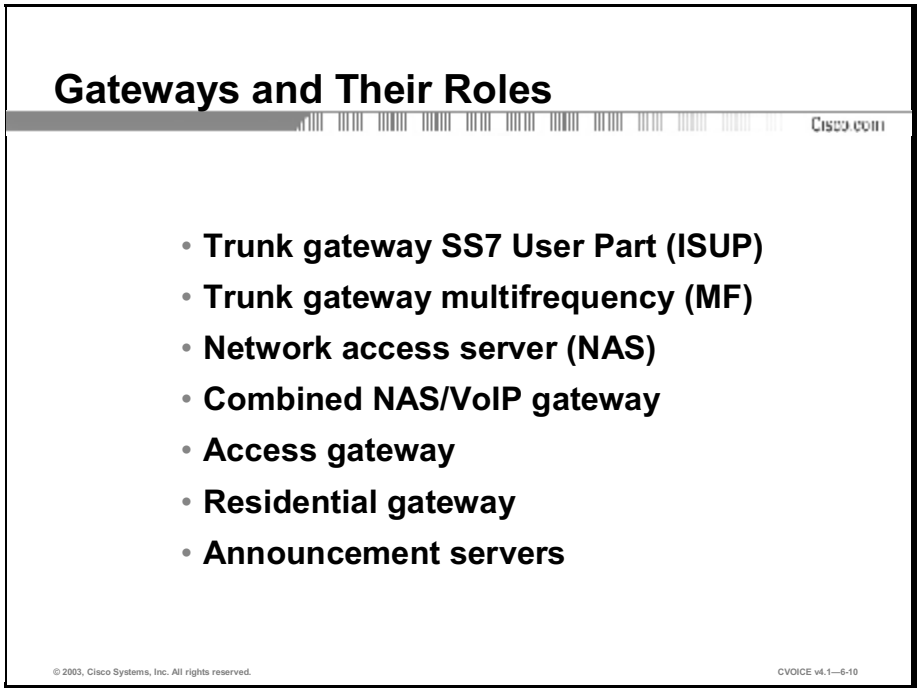
Endpoint identifiers consist of two parts: a local name of the endpoint in the context of the gateway and the domain name of the gateway itself. The two parts are separated by an “at” sign (@). If the local part represents a hierarchy, the subparts of the hierarchy are separated by a slash.

Example

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 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 the following seven types of gateways:

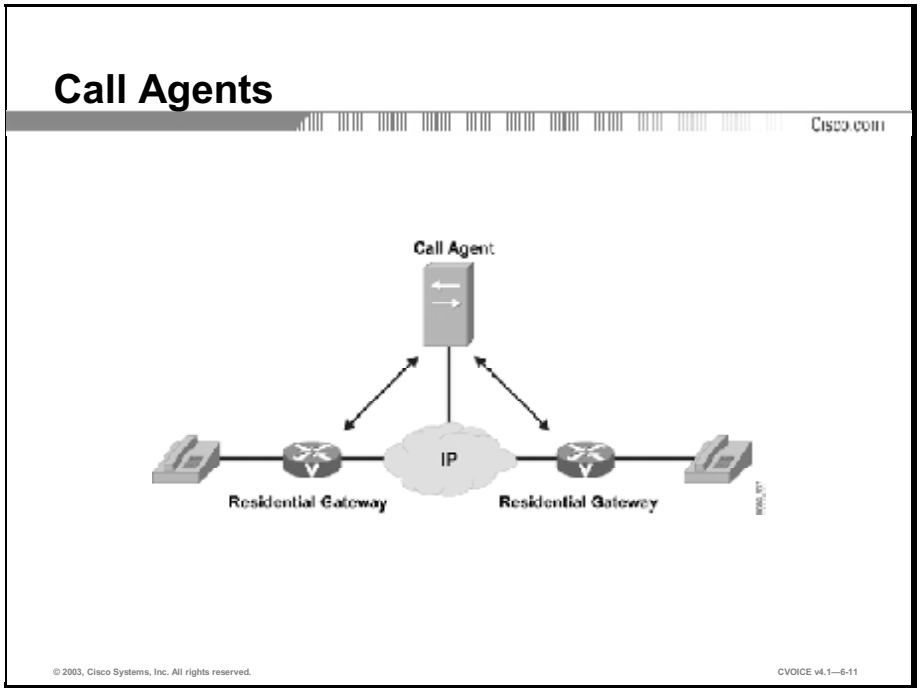
- **Trunk gateway ISDN User Part (ISUP):** Supports digital circuit endpoints subject to ISDN signaling
- **Trunk gateway multifrequency (MF):** Typically supports digital or analog circuit endpoints that are connected to a service provider of an enterprise switch that is subject to MF signaling
- **Network access server (NAS):** Supports an interconnect to endpoints over which data (modem) applications are provided
- **Combined NAS/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 server:** 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.



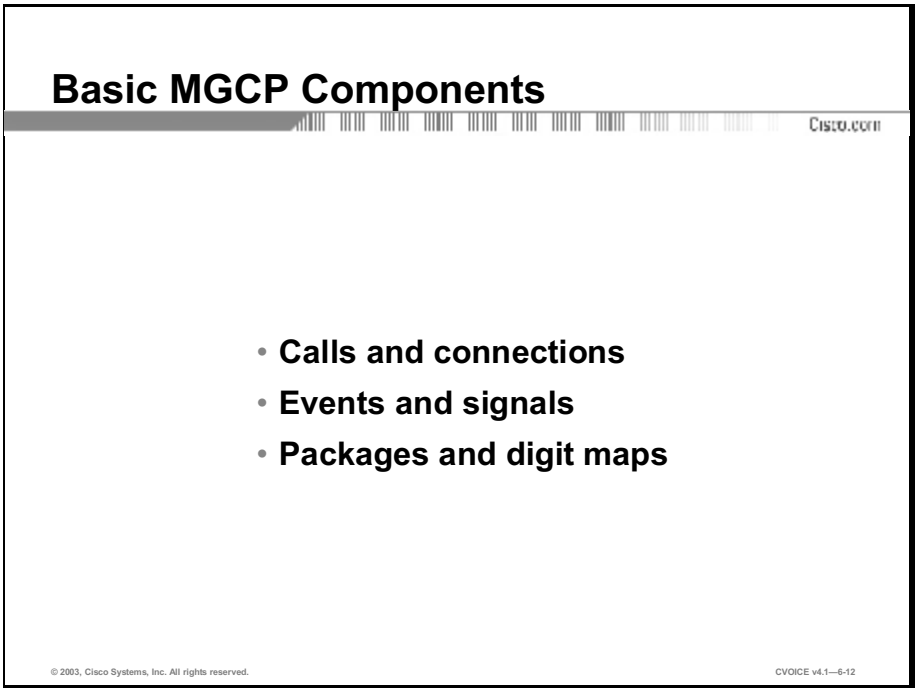
A call agent, or Media Gateway Controller (MGC), represents the central controller in an MGCP environment.

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, in addition to recognizing 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 Voice over IP (VoIP) call legs.

Basic MGCP Concepts

This topic introduces the basic MGCP concepts.

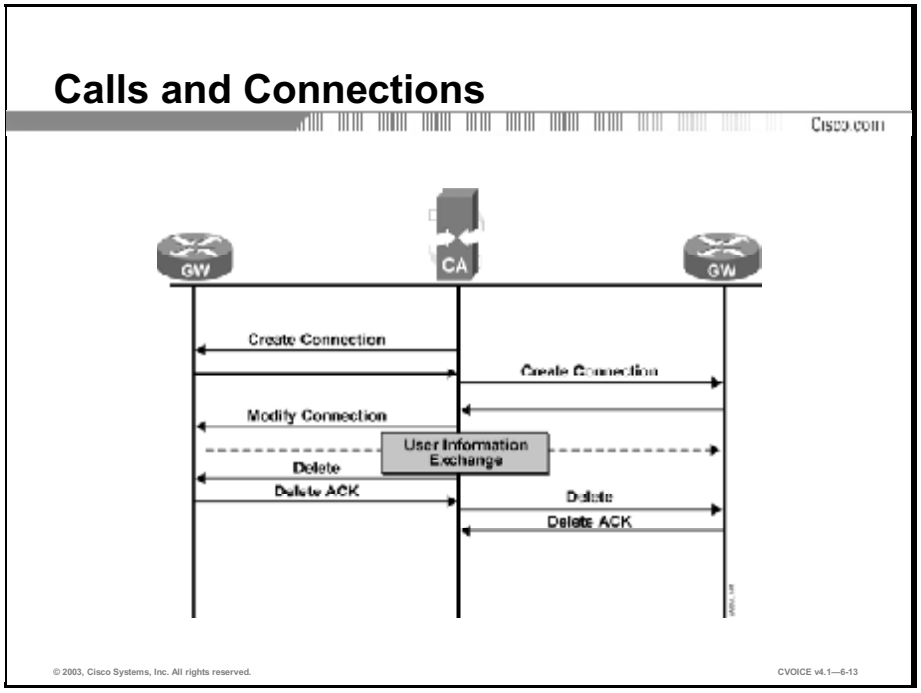


The basic MGCP concepts are listed below:

- **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

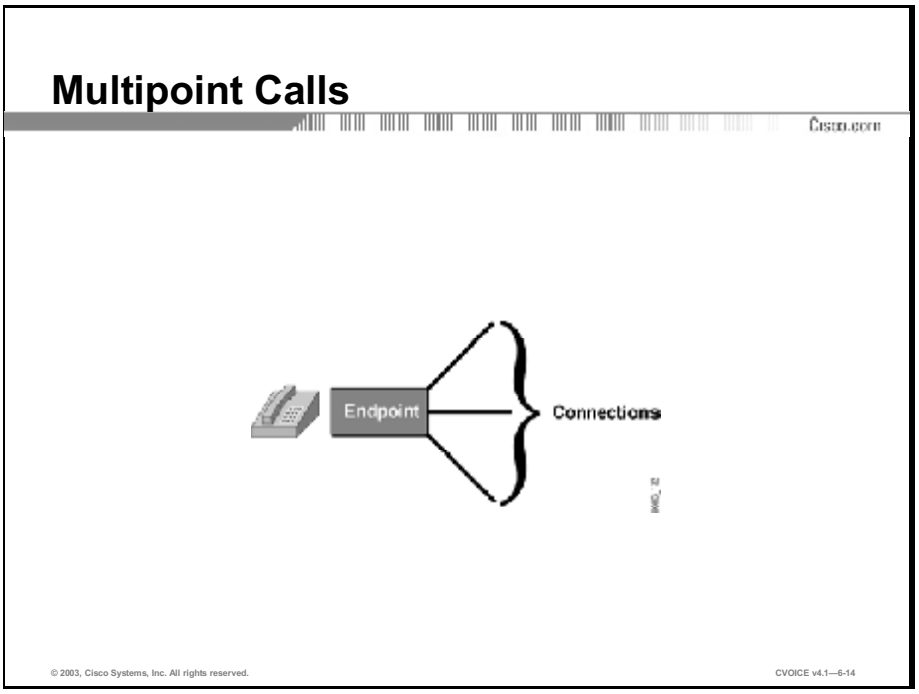
MGCP Calls and Connections

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.

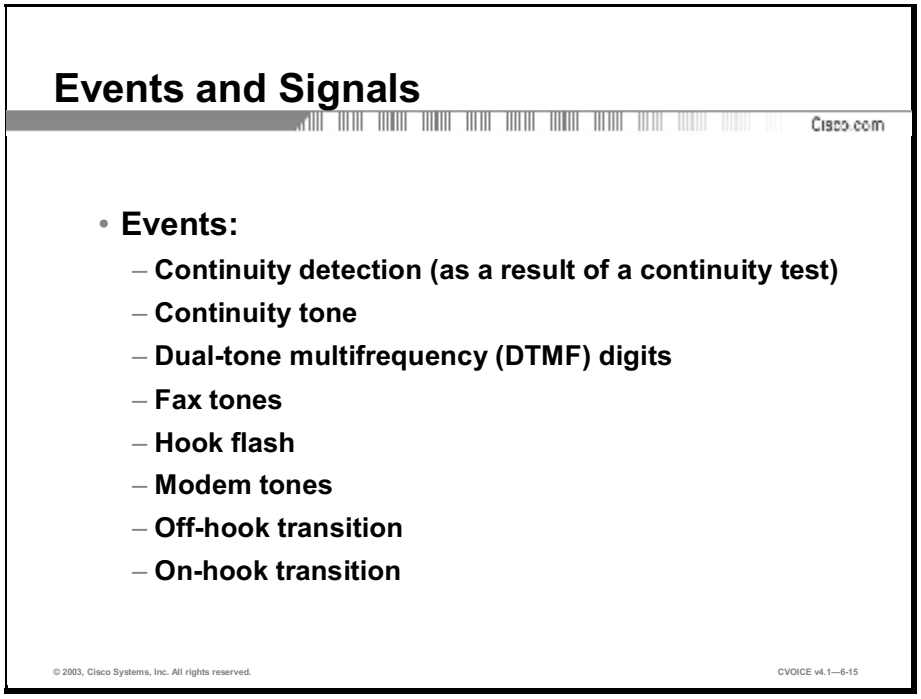
At the conclusion of a call, the call agent sends a delete connection request to each gateway.



To create a multipoint call, the call agent instructs an endpoint to create multiple connections. The endpoint is responsible for mixing audio signals.

MGCP Events and Signals

This topic describes how a call agent uses events and signals to provide instruction to the gateway.

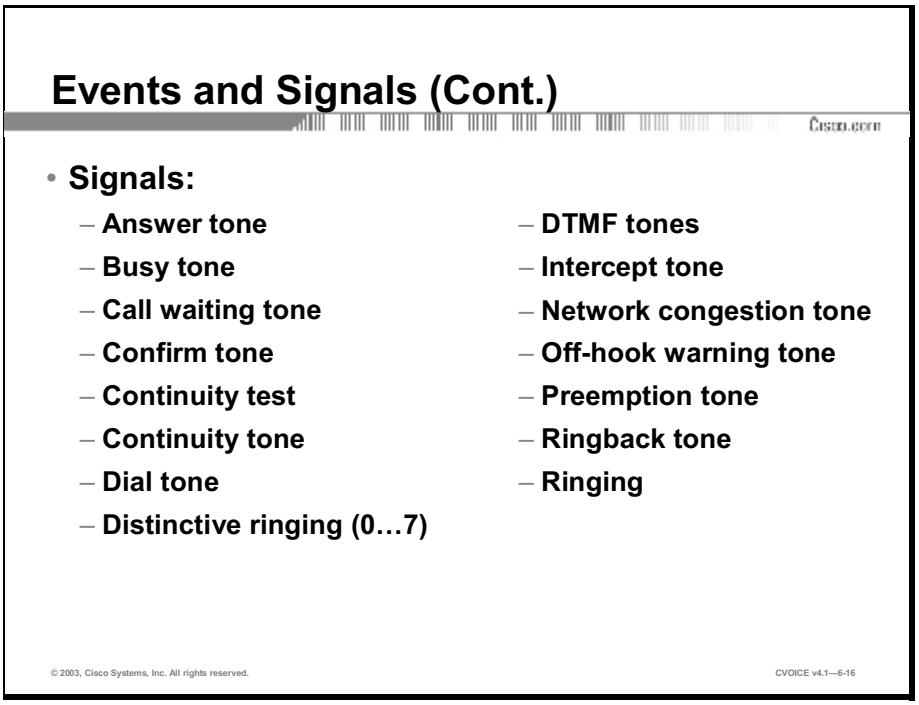


Events and signals help the call agent instruct the gateway on the basic and complicated call control and signaling procedures that are found in the telephony world. The call agent has complete control over the gateway. The call agent informs the gateway of every action to take, including the following:

- Events that the gateway monitors on an endpoint
- What to do if an event occurs
- When to generate a notification to the call agent

An example of an event on an analog line is an off-hook condition. Using signals, the call agent requests that the gateway provide dial tone upon observing the off-hook event.

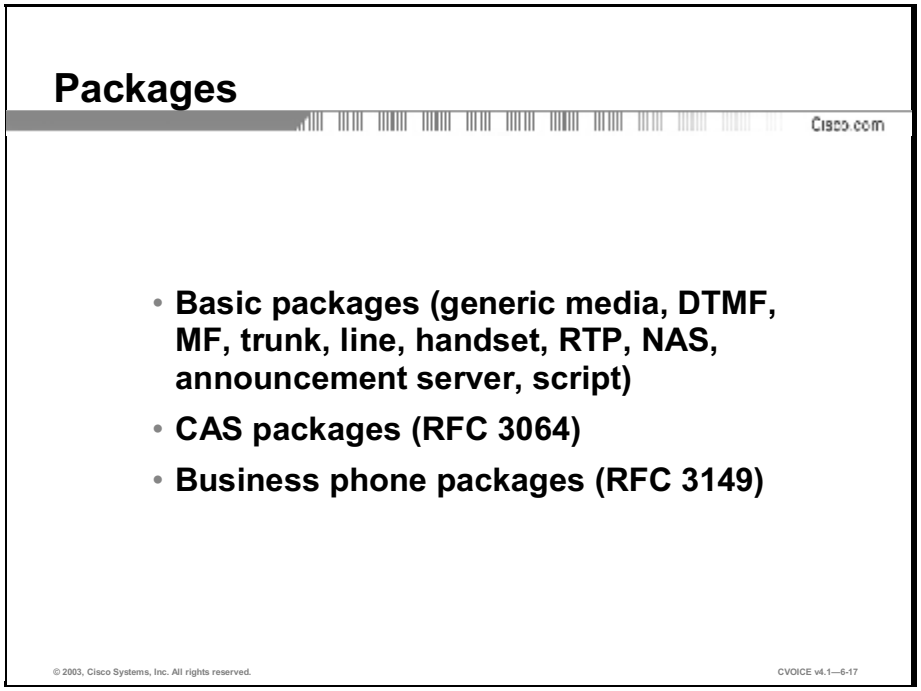
The figure lists examples of events used in MGCP environments. Events and signals are assigned simple, case-insensitive codes. For example, the code for an off-hook transition event is “hd”, and the code for the dial tone signal is “dl”.



The figure gives examples of signals used in MGCP environments.

MGCP Packages

This topic describes how events and signals are packaged in gateways and how they are used by digit maps and gateways.



Packages are collections of commonly occurring events and signals that are relevant to a specific type of endpoint. For example, “off hook,” an event, and “dial tone,” a signal, are unique to managing subscriber lines. Consequently, they are associated with the “line” package.

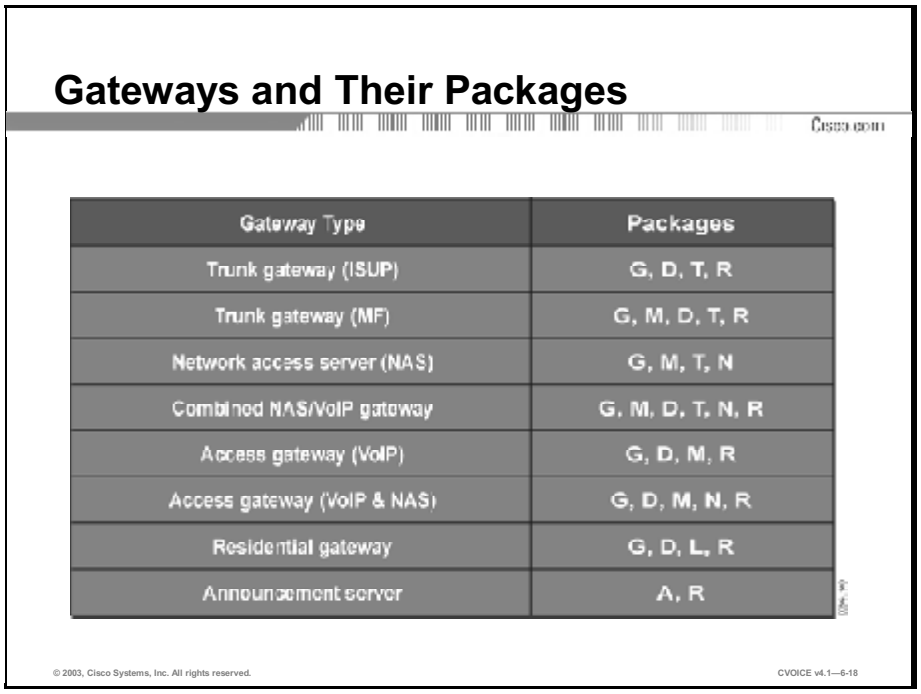
All events and signals are placed in exactly one package. The name of an event or signal acquires the code assigned to the package. The package code and the event code are separated by a slash. Therefore, the fully specified name for the off-hook transition event is “L/hd”.

RFC 2705 defines 10 packages, as shown in the table.

Table 1: Packages

Reference	Package Name
G	Generic media
M	Multifrequency
D	DTMF
T	Trunk
N	Network access server
L	Line
A	Announcement server
R	RTP
H	Handset
S	Script

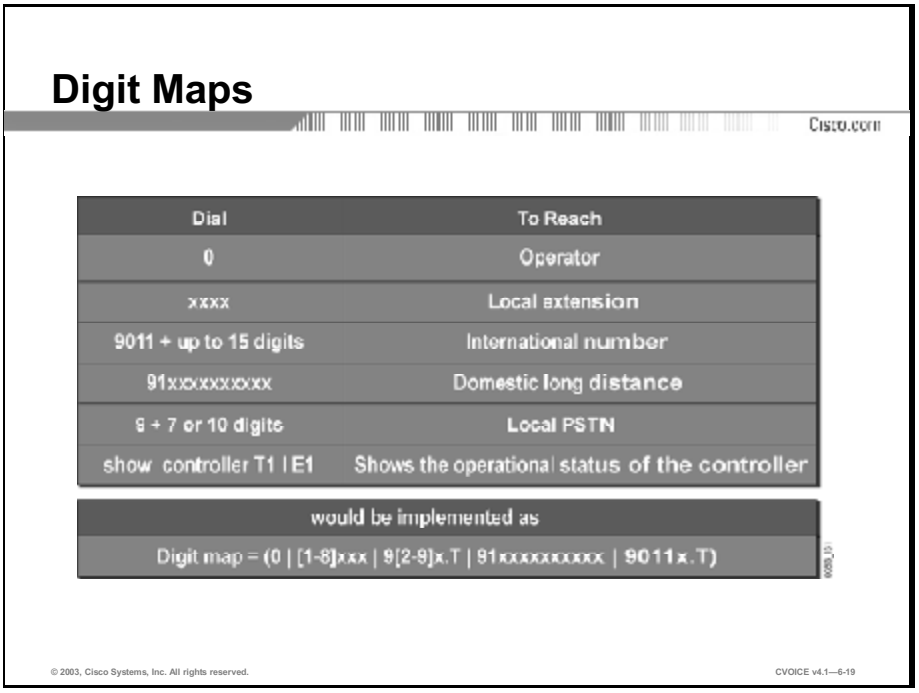
RFC 3064 defines channel associated signaling (CAS) packages, while RFC 3149 defines business telephone packages.



Packages cluster events and signals by their relevance to various types of endpoints. Conceptually, gateways also cluster endpoints of different types. It is appropriate then to associate packages with gateways. The table in the figure lists the gateways and identifies the packages that are associated with them.

MGCP Digit Maps

This topic describes the function of digit maps in MGCP.

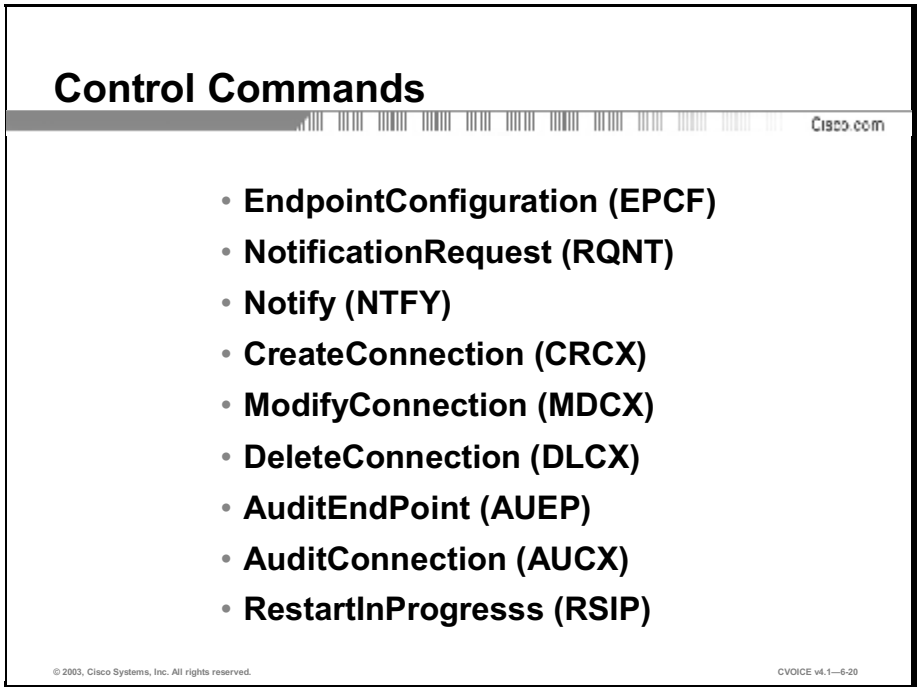


A digit map is a specification of the dial plan. When you download a digit map to a gateway for use on an endpoint or a group of endpoints, a digit map allows the gateway to collect digits until the gateway either finds a match or concludes that the dialed digits could not possibly match the specification. When either condition occurs, the gateway notifies the call agent.

Without a digit map, a gateway must notify the call agent on each digit dialed, which places a heavy burden on the call agent and the network connecting the gateway and call agent. The figure shows an example of a digit map.

MGCP Control Commands

MGCP defines nine messages to control and manage endpoints and their connections. This topic describes these control messages.



A call agent uses control commands or messages to direct its gateways and their operational behavior. Gateways use the following control commands in responding to requests from a call agent and notifying the call agent of events and abnormal behavior:

- **EndpointConfiguration (EPCF):** Identifies the coding characteristics of the endpoint interface on the line side of the gateway. The call agent issues the command.
- **NotificationRequest (RQNT):** 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):** Informs the call agent of an event for which notification was requested. The gateway issues the command.
- **CreateConnection (CRCX):** Instructs the gateway to establish a connection with an endpoint. The call agent issues the command.
- **ModifyConnection (MDCX):** Instructs the gateway to update its connection parameters for a previously established connection. The call agent issues the command.

- **DeleteConnection (DLCX):** 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.

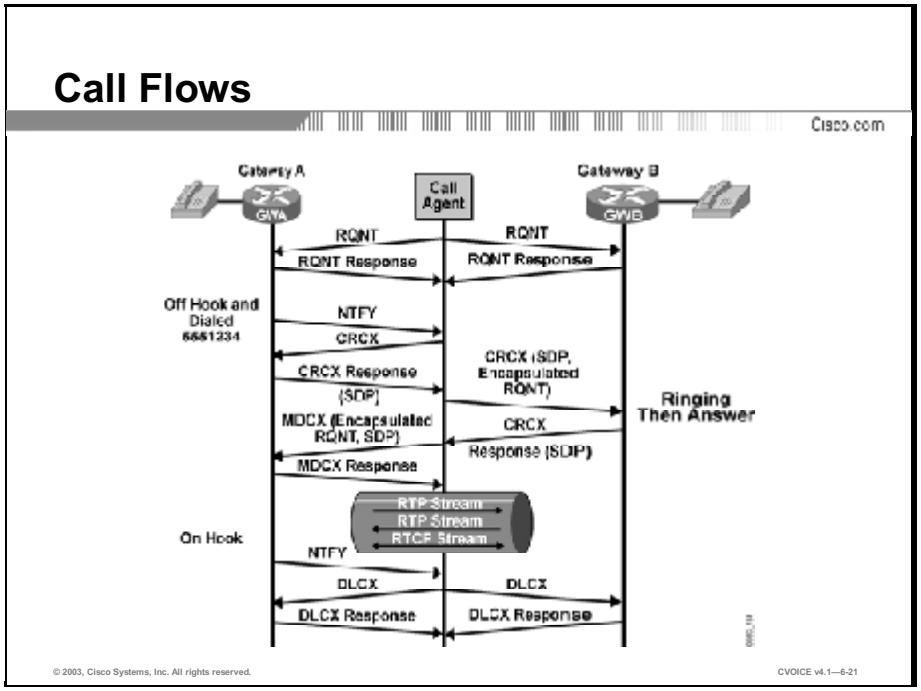
- **AuditEndpoint (AUEP):** Requests the status of an endpoint. The call agent issues the command.

- **AuditConnection (AUCX):** Requests the status of a connection. The call agent issues the command.

- **RestartInProgress (RSIP):** 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 command.

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 following principle of operation is the same for other gateway types:

1. The call agent sends a request notification (RQNT) to each gateway. Because they are residential gateways, the request instructs the gateways to wait for an off-hook transition (event). When it occurs, it also 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 a notify (NTFY) to the call agent to advise the call agent that a requested event was observed. The notify 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 on the signals and events that it should now consider relevant. In this example, where 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 a modify connection request (MDCX). This request may contain an encapsulated notify request that describes the relevant signals and events at this stage of the call setup. Now gateway A and gateway B have the required session descriptions to establish the RTP sessions over which the audio travels.

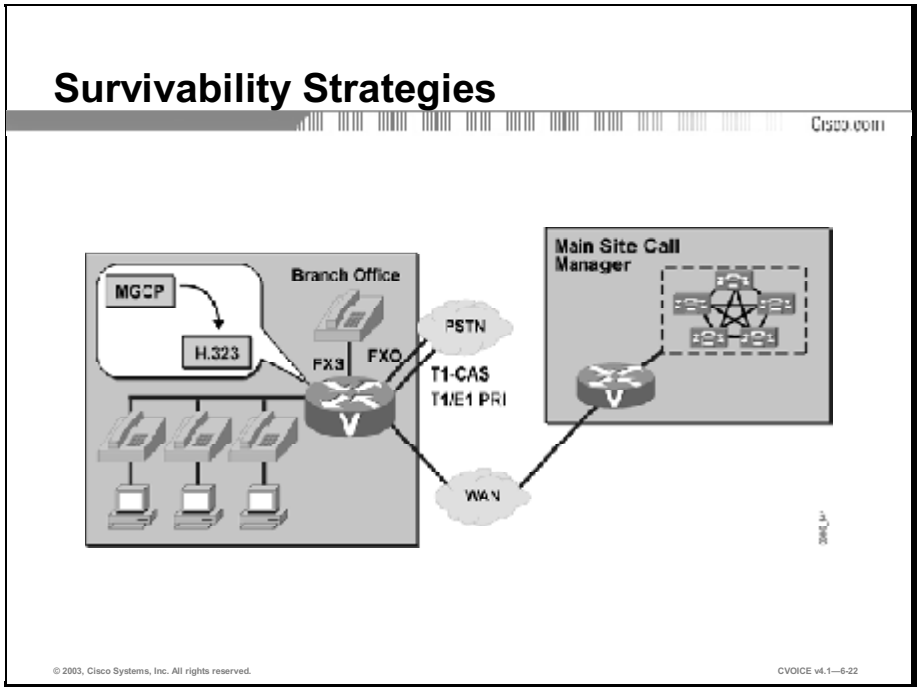
10. At the conclusion of the call, one of the endpoints recognizes an on-hook transition. In the example, the user on gateway A hangs up. Because the call agent requested the gateways to notify in such an event, gateway A notifies the call agent.

11. The call agent sends a delete connection (DLCX) request to each gateway.

12. The gateways delete the connections and respond.

Survivability Strategies

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 following manner:

- **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 for a specified period, it tries to establish a new connection with a backup Cisco CallManager server.

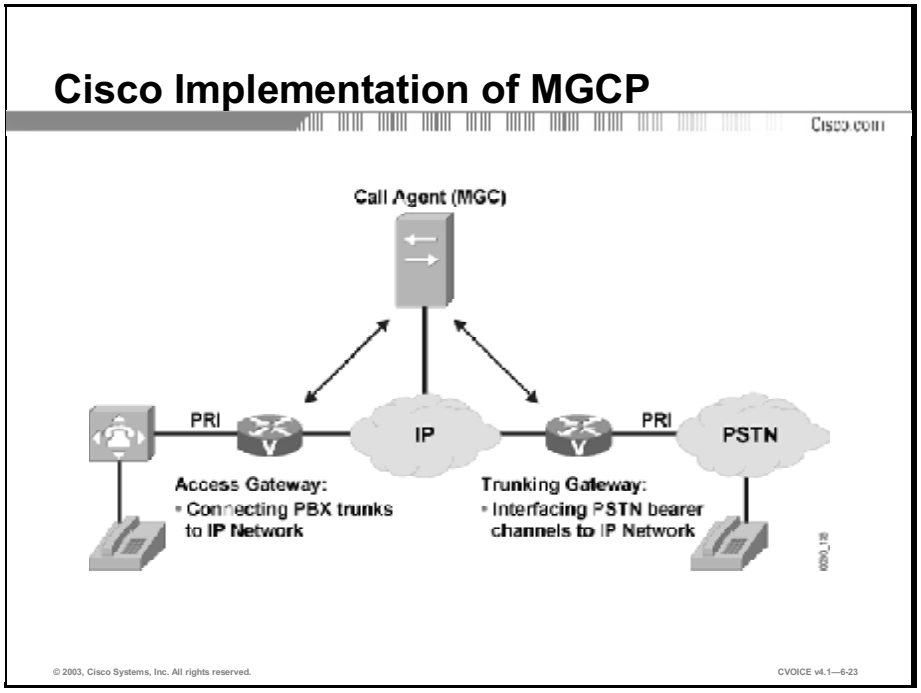
You can configure a Cisco voice gateway to reestablish connection with the primary Cisco CallManager server when it becomes available again. This is the switchback function.

- **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 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 is unavailable.

Cisco Implementation of MGCP

This topic describes how Cisco implements MGCP.



Cisco provides support for MGCP gateways and the call agent in the following way:

- **Gateways:** Cisco implements MGCP trunk gateway and residential gateway support in the following devices:
  - Cisco voice-enabled routers (first available in Cisco IOS® release 12.1)
  - Cisco PGW 2200 public switched telephone network (PSTN) gateways
  - Cisco VG200
  - Voice-enabled AS5xx0 access servers
  - BTS 10200 Softswitch

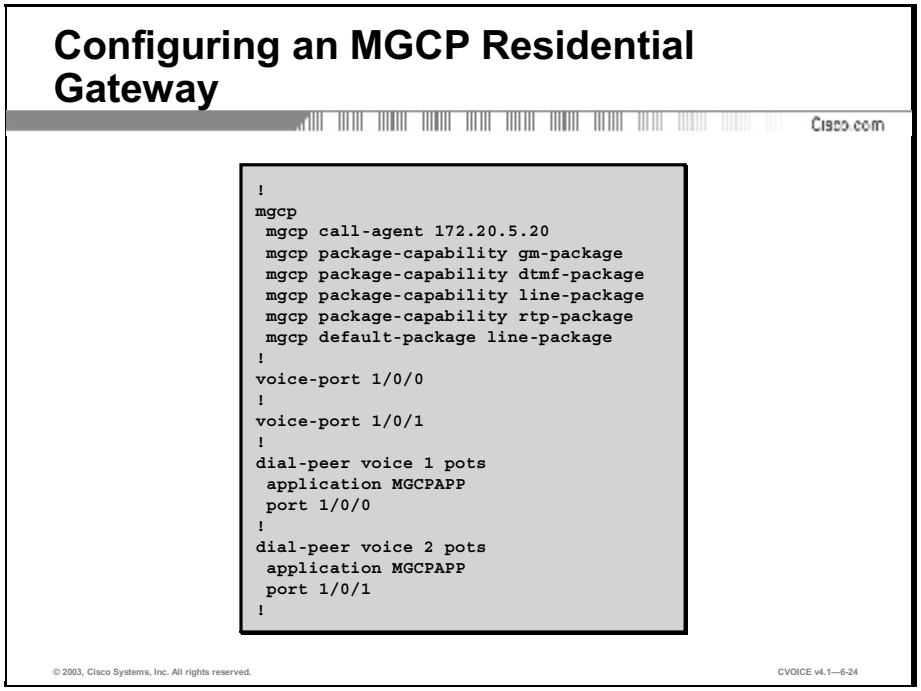
Note	Cisco CallManager interworking requires Cisco IOS release 12.2.

- **Call agent:** Cisco implements call agent support in the following applications:
  - Cisco CallManager
  - 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 Connection Online (CCO) 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, then 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.

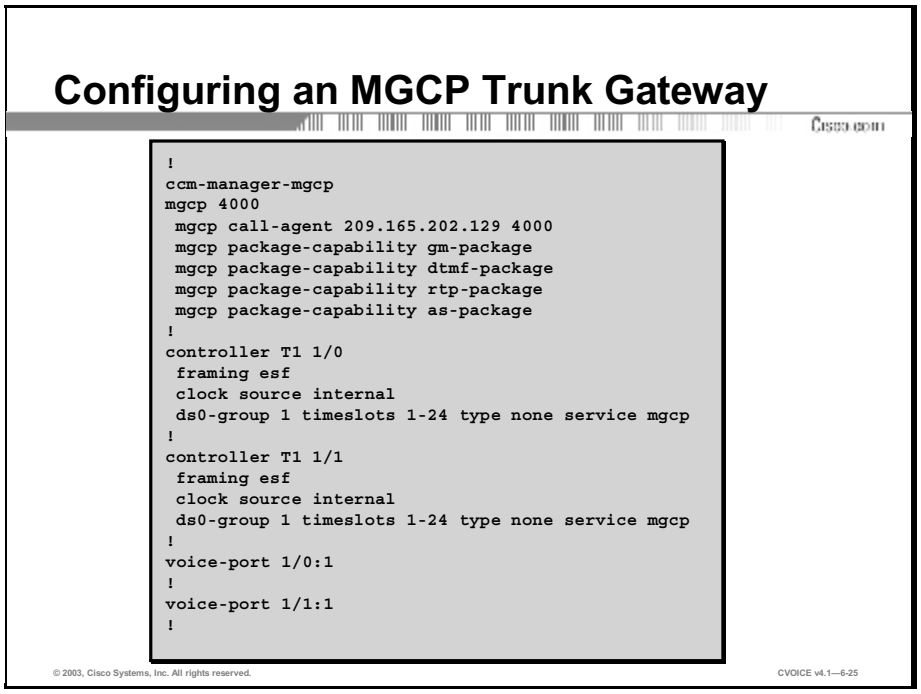
At least one **mgcp call-agent** command is required below the **mgcp** command. This command indicates the location of the call agent. The command identifies the call agent by an IP address or a host name. Using a host name adds a measure of fault tolerance in a network that has multiple call agents. 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

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 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.

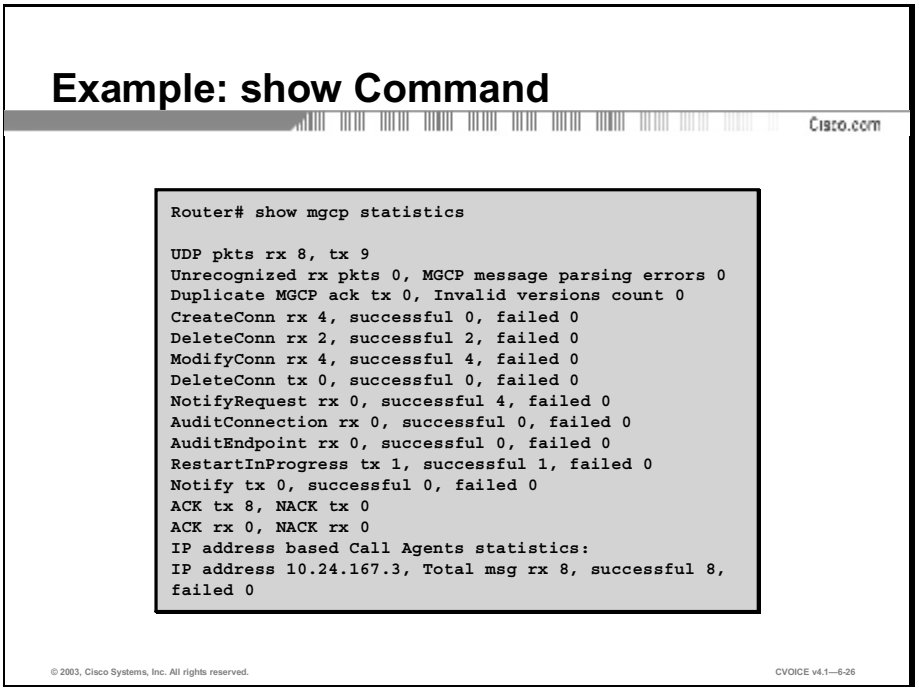
Configuring trunk gateways requires the address or the name of the call agent, which is a requirement common to a residential gateway (RGW). The trunk package is the default for a trunk gateway and does not need to be configured. Again, other parameters are optional.

Example

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 MGCP

Several **show** and **debug** commands provide support for monitoring and troubleshooting MGCP. This topic lists many useful **show** and **debug** commands.



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 in each and how this information can help you.

The following **show** commands are useful for monitoring and troubleshooting MGCP:

- **show call active voice [brief]:** 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]:** Displays call records from the history buffer.
- **show mgcp:** Displays basic configuration information about the gateway.
- **show mgcp connection:** Displays details of the current connections.
- **show mgcp endpoint:** Displays a list of the voice ports that are configured for MGCP.
- **show mgcp statistics:** Displays a count of the successful and unsuccessful control commands (shown in the figure). You should investigate a high unsuccessful count.

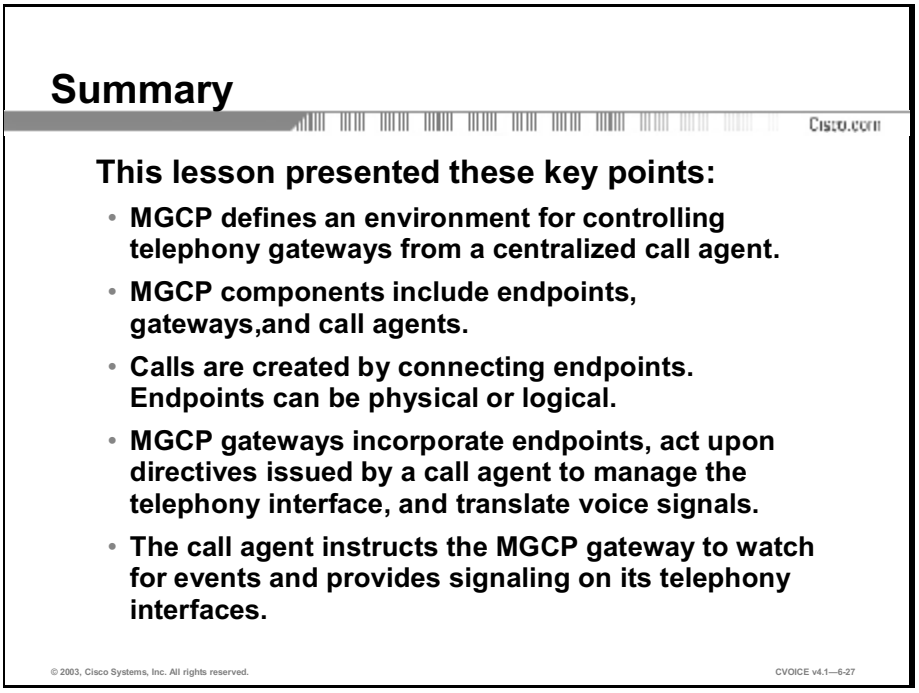
The following **debug** commands are useful for monitoring and troubleshooting MGCP:

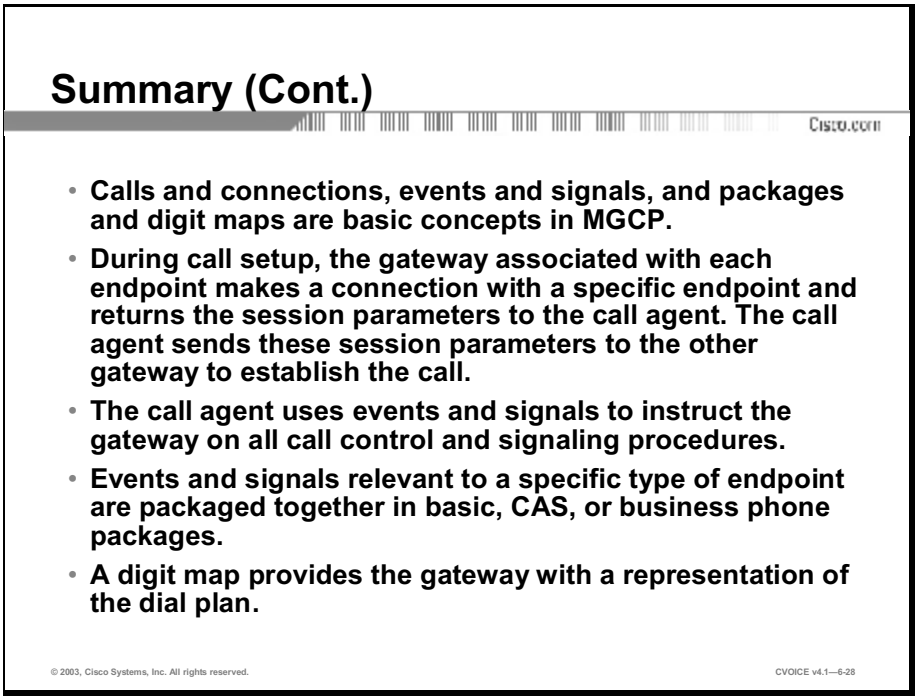
- **debug voip ccapi inout:** Shows every interaction with the call control application program interface (API) on the telephone interface and the VoIP side. Watching the output allows users to follow the progress of a call from the inbound interface or VoIP peer to the outbound side of the call. This debug is very active; you must use it sparingly in a live network.

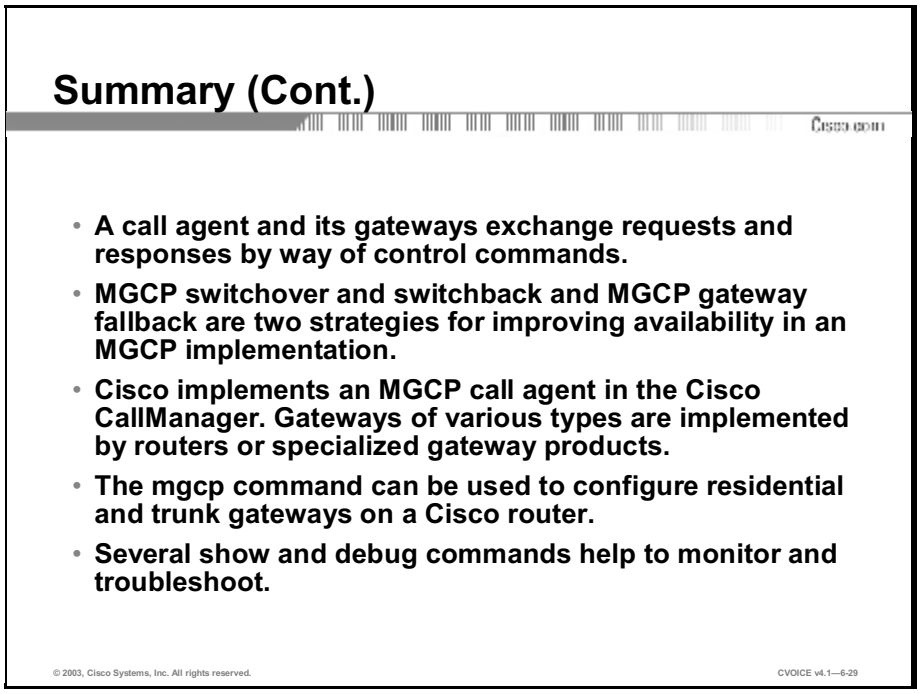
- **debug mgcp [all | errors | events | packets | parser]:** Reports all **mgcp** command activity. You must use this debug to trace the MGCP request and responses.

Summary

This topic summarizes the key points discussed in this lesson.







Next Steps

After completing this lesson, go to:

- Assessment (Quiz): MGCP
- Assessment (Complex Lab): Refer to Lab 6-3, contained in Laboratory Exercises in Additional Resources section E.
- Comparing Call Control Models lesson

References

For additional information, refer to these resources:

- “IETF RFC 2705: Media Gateway Control Protocol (MGCP), version 1.0”
- “IETF RFC 2805: Media Gateway Control Protocol Architecture and Requirements”
- “Cisco IOS Voice, Video, and Fax Configuration Guide”
- “Cisco IOS Voice, Video, and Fax Command Reference”

Quiz: MGCP

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Define MGCP and its functions
- List the basic components of MGCP
- Name eight types of MGCP endpoints defined in RFC 2705 and identify their functions
- Name seven types of MGCP gateways defined in RFC 2705 and identify their functions
- Describe the function of a call agent in an MGCP environment
- List the basic concepts of MGCP
- List the steps involved in the process of MGCP call establishment
- Describe the function of MGCP events and signals and give five examples of each
- List eight types of MGCP gateways and the packages that are associated with each gateway
- Explain how digit maps reduce the load on the network during call setup
- List nine MGCP control messages that are used to control and manage endpoints and their connections
- Describe MGCP call setup and control procedures
- Identify two strategies implemented by Cisco Systems to provide high availability in an MGCP environment
- Identify the Cisco devices that implement MGCP
- Use the **mgcp** command and subcommands to configure an MGCP residential and trunk gateway on a Cisco router
- Use **show** and **debug** commands to monitor and troubleshoot MGCP

Instructions

Answer these questions.

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) to handle the translation of video between the SCN and the packet-switched network

B) to handle the translation of audio between the SCN and the packet-switched network

C) to control the operation of the endpoints and the call agent

D) to allow only authenticated traffic into the network

Q5) According to RFC 2705, which type of MGCP endpoint represents an access 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) How many call agents can an MGCP gateway interact with?

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 the MGCP require the gateway to observe and report events?

A) so that it can recognize each endpoint that it supports

B) so that it can tell the endpoint what type of signal to send to the attached telephone equipment

C) so that it can recognize the signaling characteristics of each physical interface attached to the gateway

D) so that it can recognize the signaling characteristics of each logical interface attached to the gateway

Q10) What two pieces of information does the MGC 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) What two components 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) What two components 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) end point

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) Which two examples represent MGCP events? (Choose two.)

A) busy tone

B) continuity test

C) distinctive ringing

D) fax tones

E) hook flash

F) ringing

Q16) Which two examples represent MGCP signals? (Choose two.)

A) confirm tone

B) continuity detection

C) continuity test

D) DTMF digits

E) on-hook transition

Q17) Which two packages are associated with the NAS? (Choose two.)

A) multifrequency

B) DTMF

C) trunk

D) line

E) announcement server

F) RTP

Q18) Which two packages are associated with the residential gateway? (Choose three.)

A) generic media

B) multifrequency

C) DTMF

D) trunk

E) network access server

F) line

Q19) A gateway that is using a digit map notifies the call agent when _____. (Choose two.)

A) each digit is collected

B) all the digits have been collected

C) the gateway finds a match for the digits

D) the digits that match the area code have been collected

E) the gateway concludes that the dialed digits cannot be matched

Q20) In the United States, how would the digit map identify digits for the local PSTN?

A) xxxx

B) 91xxxxxxxxx

C) 9 + 7 or 10 digits

D) 9011 + up to 15 digits

Q21) Match the MGCP control command 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 upon 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

Q22) Which two commands are issued by a gateway? (Choose two.)

A) EndpointConfiguration

B) NotificationRequest

C) CreateConnection

D) DeleteConnection

E) RestartInProgress

Q23) Which two types of information are included in the notify (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

Q24) 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

Q25) 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.

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 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.

Q26) 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) BTS 10200 Softswitch

Q27) 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) BTS 10200 Softswitch

Q28) 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 Gateway

D) BTS 10200 Softswitch

Q29) 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

Q30) 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.

Q31) 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**

Q32) 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**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

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.

Importance

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:

- Compare the features and benefits of H.323, SIP, and MGCP
- Describe the environments best suited to H.323, SIP, and MGCP

Learner Skills and Knowledge

To fully benefit 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 Voice over IP (VoIP)
- An understanding of the H.323, SIP, and MGCP call control models

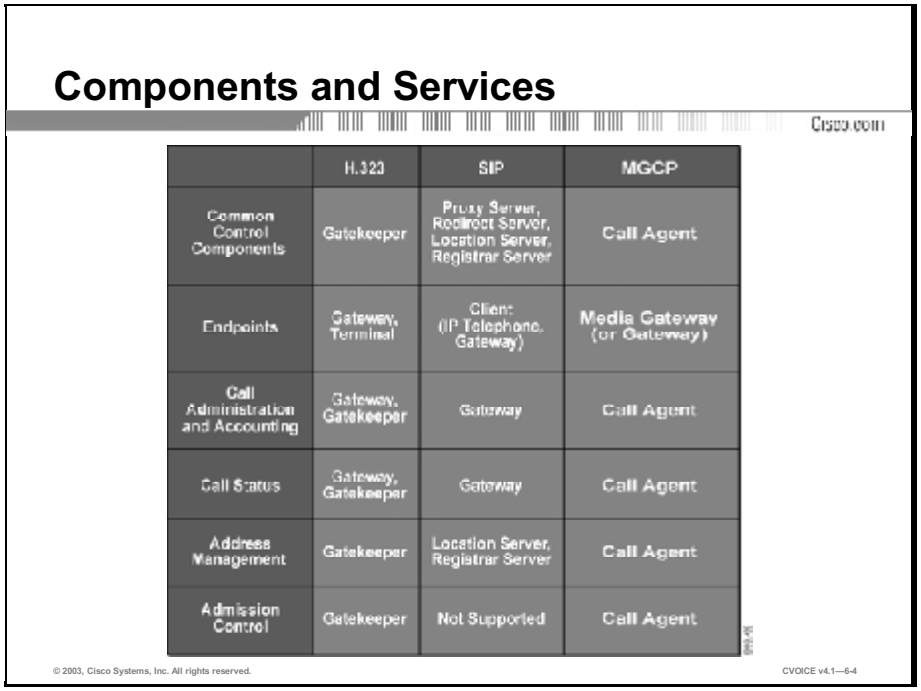
Outline

This lesson includes these topics:

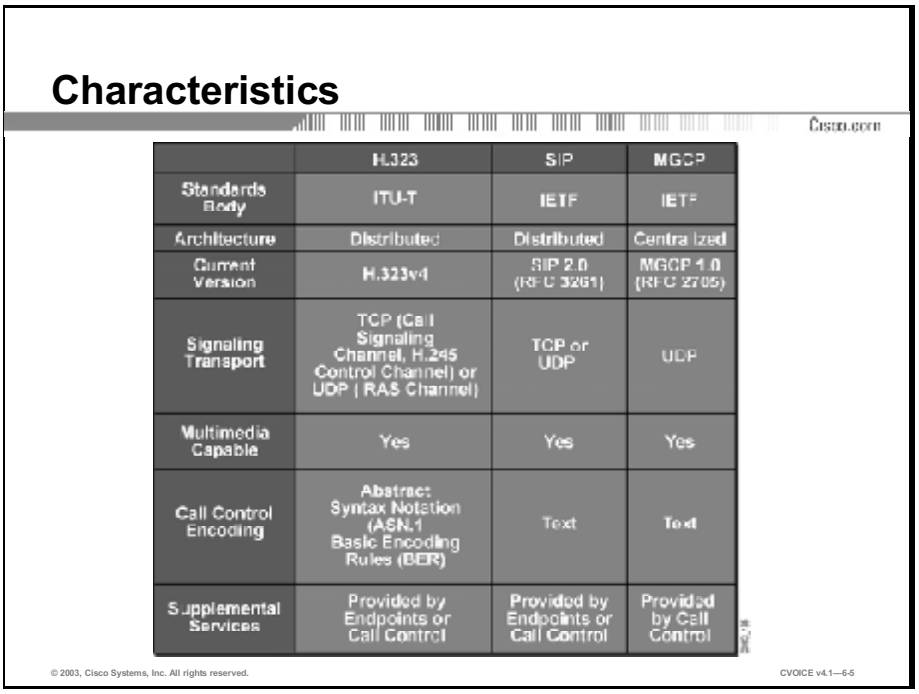
- Overview
- Feature Comparison Charts
- Strengths of H.323, SIP, and MGCP
- Summary
- Assessment (Quiz): Comparing Call Control Models

Feature Comparison Charts

This topic compares the origins, architectures, characteristics, and capabilities of the H.323, session initiation protocol (SIP), and Media Gateway Control Protocol (MGCP) call control models.



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.



Note As of version 3 of H.323, the calling signaling channel, and the H.245 control channel can be UDP based.

The chart in the figure compares several factors that can influence your decision to select H.323, SIP, or MGCP.

Standards Bodies (ITU-T versus IETF)

The two originating authorities for the model may seem to have little relevance. However, the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the Internet Engineering Task Force (IETF) work under different conditions, which have 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 are 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 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 versus Distributed)

The distinction between the two 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 versus 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, User Datagram Protocol (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.

Call Control Encoding (ASN.1 versus 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.

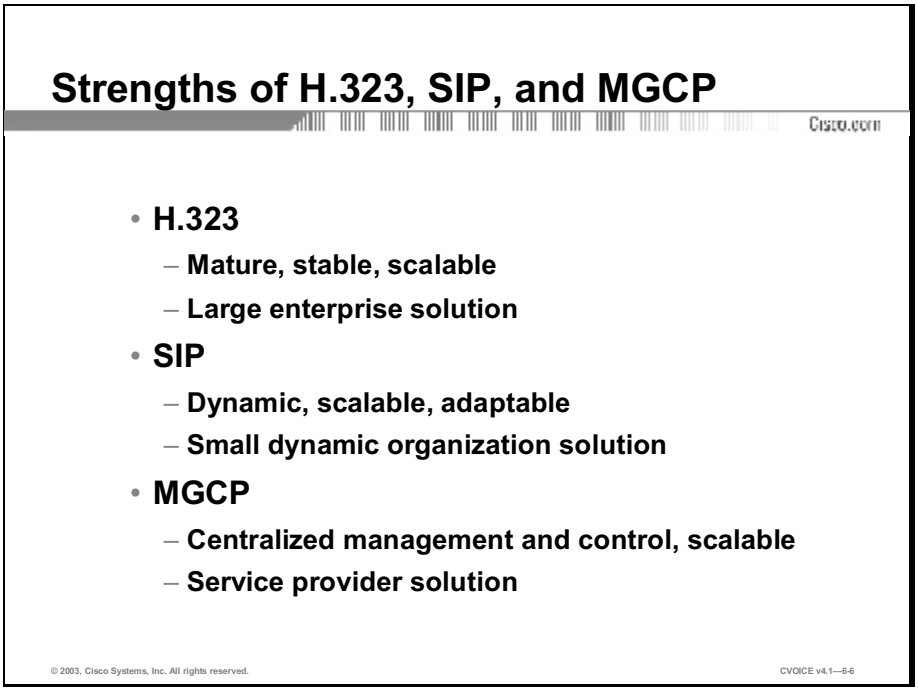
Supplementary Services (Endpoint versus Call Control)

Where and how you introduce supplementary services can be important considerations.

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.



H.323

H.323, the only viable option in 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 operations, administration, and maintenance (OA&M).

SIP

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 small, dynamic organizations and Internet service providers.

MGCP

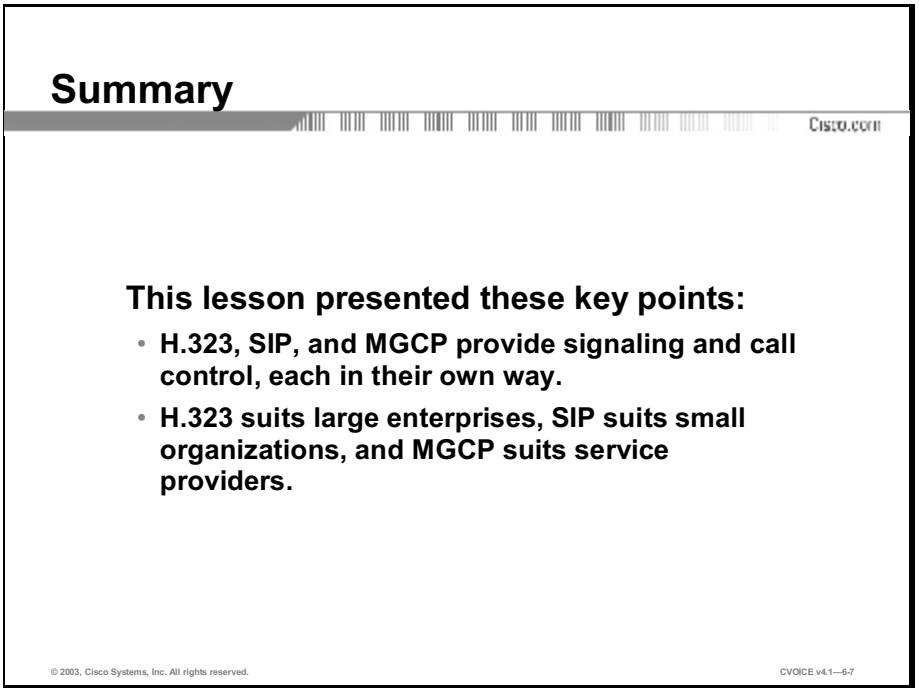
MGCP describes an architecture where call control and services such as OA&M is centrally added to a VoIP network. As a result, MGCP architecture closely resembles the existing public switched telephone network (PSTN) architecture and services.

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.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Lesson Assessment (Quiz): Comparing Call Control Models
- Improving and Maintaining Voice Quality module

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”

Quiz: Comparing Call Control Models

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Compare the features and benefits of H.323, SIP, and MGCP
- Describe the environments best suited to H.323, SIP, and MGCP

Instructions

Answer these questions:

Q1) Which call control model uses encoding that 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. Each call control model can be used more than once.

A) client

B) terminal

C) gateway

D) media gateway

_____ 1. H.323

_____ 2. SIP

_____ 3. MGCP

Q3) Which call control model most closely resembles the PSTN?

A) H.323

B) SGCP

C) SIP

D) MGCP

Q4) Which call control model is popular in large enterprises because of its maturity and stability?

A) H.323

B) SGCP

C) SIP

D) MGCP

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 100 percent.

7

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.

Upon completing this module, you will be able to:

- Provide voice quality on a network, given Perceptual Speech Quality Measurement and mean opinion score as tools for measuring voice quality
- Implement a converged voice and data IP network, given the challenges of delivering voice packets on an IP internetwork
- Design a voice network that operates optimally, given the educational resources provided by Cisco Systems for network administrators
- Configure buffers for static and dynamic jitter, given the conditions that require jitter buffers
- Calculate, minimize, and verify delay on Cisco routers, given the factors that contribute to delay on a network
- Configure quality of service features on a campus network, given the requirements of separating and scheduling

- Configure Voice over IP over Frame Relay and Voice over IP over Point-to-Point Protocol, given the QoS components particular to each technology
- Configure call control on the network, given the characteristics of Call Admission Control tools
- Allocate bandwidth for voice and data traffic, given traffic statistics and network objectives

Outline

The module contains these lessons:

- Voice Quality Measurement
- VoIP Challenges
- QoS and Good Design
- Understanding Jitter
- Understanding Delay
- Applying QoS in a Campus Network
- Applying QoS in a WAN
- Call Admission Control
- Voice Bandwidth Engineering

Voice Quality Measurement

Overview

As technology invents and reinvents new ways to electronically represent the human voice, a method to compare the quality of each representation is necessary. Two quality measurement techniques are mean opinion score (MOS) and Perceptual Speech Quality Measurement (PSQM). In this lesson, you will learn the details of these two measurement techniques and the scores attained with different compression methods.

Importance

To understand more about the tools that you must use to improve voice quality of service (QoS), you must be knowledgeable about how voice quality is measured and how it is affected.

Objectives

Upon completing this lesson, you will be able to:

- List the attributes that affect audio clarity
- Describe the psychological comfort factors that affect voice quality
- State the purpose of MOS and the method used to calculate it
- State the purpose of PSQM and the method used to calculate it
- Describe how the voice quality score differences between various coder-decoder examples is measured

Learner Skills and Knowledge

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

- Knowledge of voice telephony systems, including traditional and Voice over IP (VoIP)
- Knowledge of Cisco IOS® software

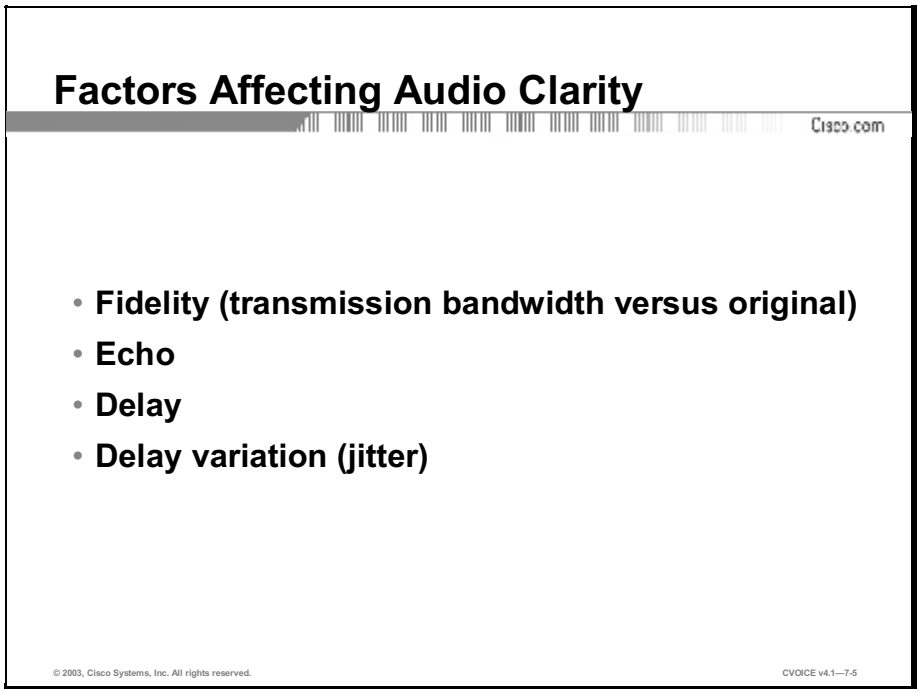
Outline

This lesson includes these topics:

- Overview
- Audio Clarity
- Comfort Factors
- MOS
- PSQM
- Comparison of Codec Quality Scores
- Summary
- Assessment (Quiz): Voice Quality Measurement

Audio Clarity

The effectiveness of a telephone conversation depends on its clarity. If the conversation does not sound good, the listener is annoyed and the speaker is unable to express the message. The clarity of the conversation must be maintained end to end, from the speaker to the listener. This topic lists the factors affecting audio clarity.



The clarity (or cleanliness and crispness) of the audio signal is of utmost importance. The listener should recognize the identity of the speaker and sense the "mood" of the speaker. This is accomplished by maintaining the clarity of the spoken voice. Factors that can affect clarity include:

- **Fidelity:** Consistency of transmission bandwidth to the original bandwidth. 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.

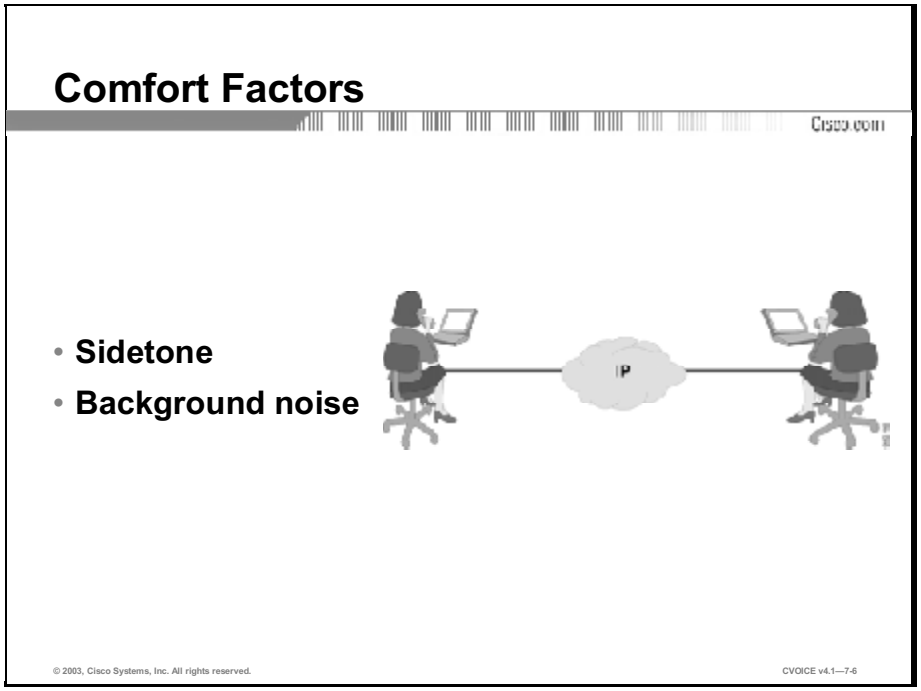
- **Echo:** A result of electrical impedance mismatches in the transmission path. Echo is always present. The two components that affect echo are amplitude (loudness of the echo) and delay (the time between the spoken voice and the echoed sound). You can control echo using suppressors or cancellers.

- **Delay:** The time between the spoken voice and the arrival of the electronically delivered voice at the far end. Delay is affected by a number of factors, including distance (propagation delay), coding, compression, serialization, and buffers.

- **Delay variation:** Because of the nature of an IP delivery network, the arrival of coded speech at the far end of a Voice over IP (VoIP) network can vary. 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 cause the listener great annoyance. Delay is induced in the network if you vary the routes of individual packets, contention, or congestion. You can solve variable delay by using dejitter buffers.

Comfort Factors

In addition to audio clarity, a number of psychological comfort factors affect the perceived quality of voice. Together these factors can cause the listener to rate the overall quality as good or poor. This topic lists these psychological factors.



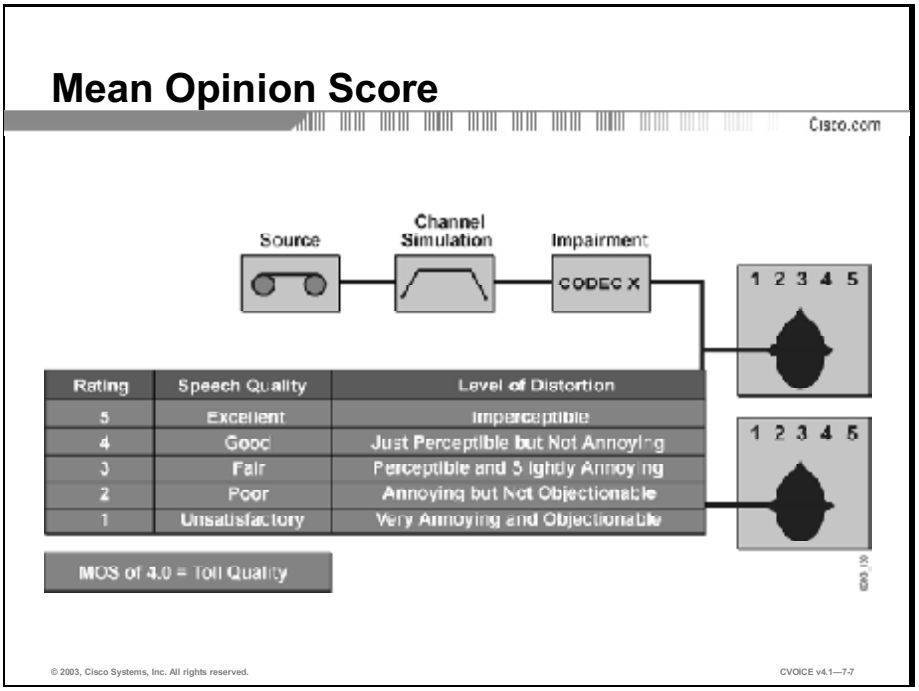
When transporting VoIP, the perceived quality of the received voice must mimic the traditional public switched telephone network (PSTN). There should be no perceived differences. The following two comfort factors affect quality:

- **Sidetone:** 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:** 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 the speaker thinks the connection is broken because nothing is heard in the earpiece from the far end.

Mean Opinion Score

This topic explains calculating mean opinion score (MOS) and using MOS to compare voice quality.

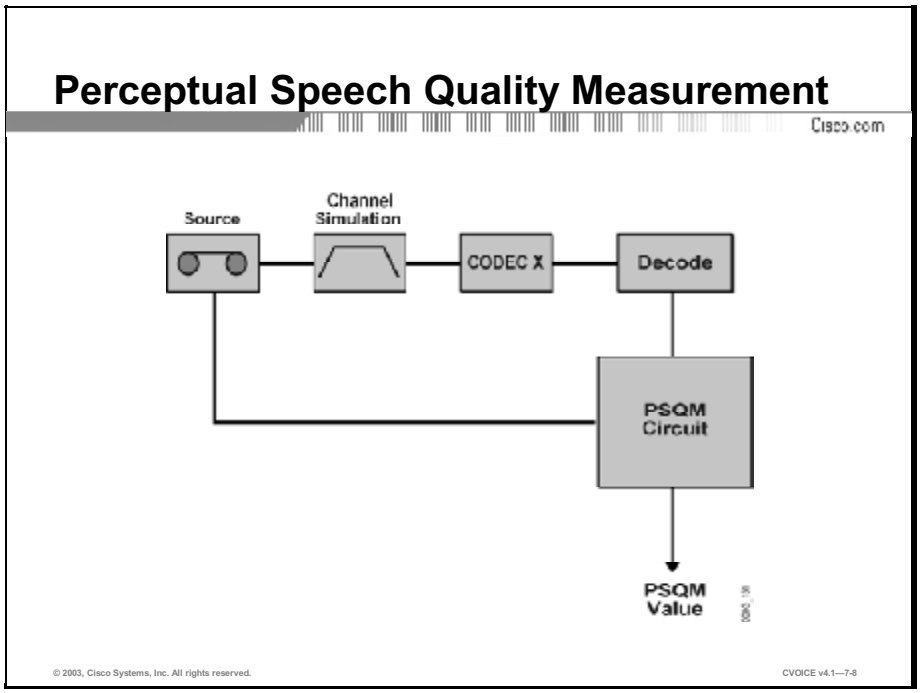


MOS is a scoring system for voice quality. An MOS score is generated when listeners evaluate prerecorded sentences that are subject to varying conditions, such as compression algorithms. Listeners then assign the sentences values, based on a scale from 1 to 5, where 1 is the worst and 5 is the best, as shown in the figure. 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 using G.711 as a baseline, so that the scores can be normalized and compared directly.

Perceptual Speech Quality Measurement

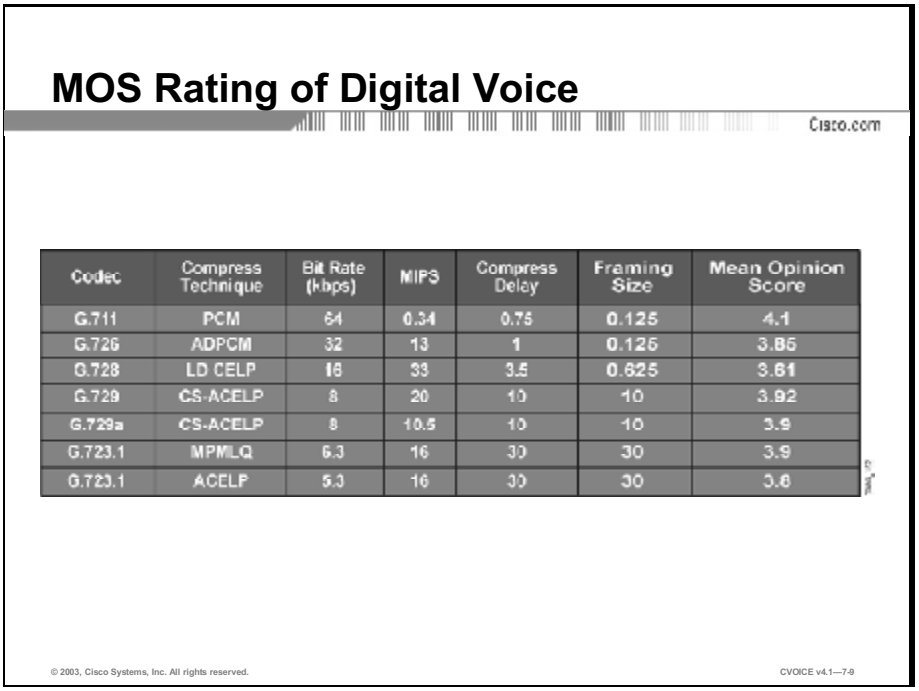
Perceptual Speech Quality Measurement (PSQM) is an automated method of measuring speech quality “in-service” or as it happens. PSQM software usually resides with IP call management systems, which are sometimes integrated into Simple Network Management Protocol (SNMP) systems. This topic describes PSQM calculations.



Equipment and software that can measure PSQM is available through third-party vendors; it is not implemented in Cisco Systems equipment. The measurement is made by comparing the original transmitted speech to the resulting speech at the far end of the transmission channel, as displayed in the figure. PSQM systems are deployed as either “in-service” or real time. The PSQM measurements are made during real conversation on the network. This automated testing algorithm has over 90 percent accuracy compared to the actual 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.

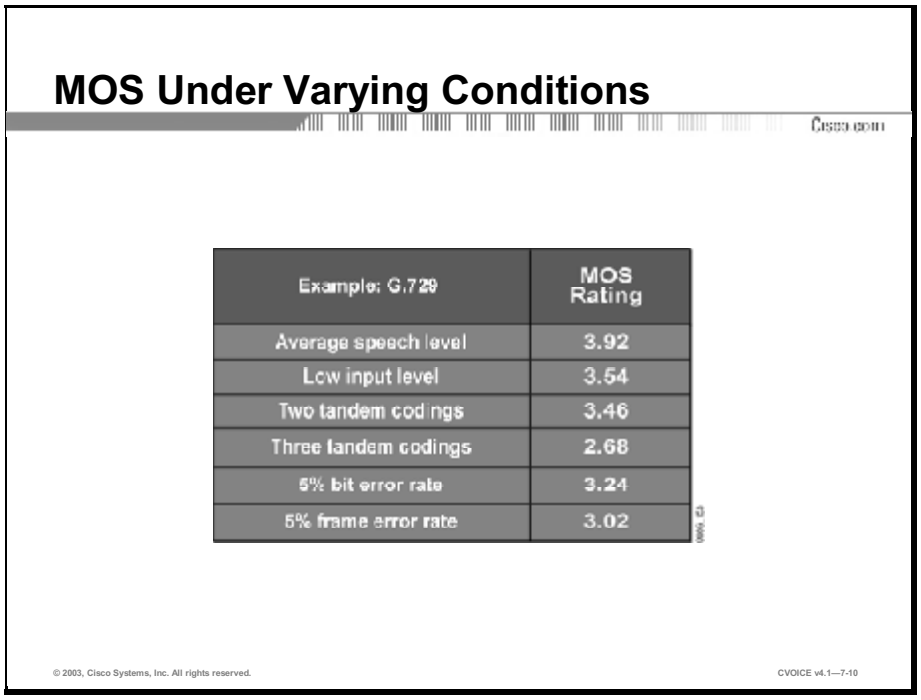
Comparison of Codec Quality Scores

This topic provides a relative comparison of scores from various coding and compression schemes.



Codec	Compress Technique	Bit Rate (kbps)	MIPS	Compress Delay	Framing Size	Mean Opinion Score
G.711	PCM	64	0.34	0.75	0.125	4.1
G.726	ADPCM	32	13	1	0.125	3.85
G.728	LD CELP	16	33	3.5	0.625	3.61
G.729	CS-ACELP	8	20	10	10	3.92
G.729a	CS-ACELP	8	10.5	10	10	3.9
G.723.1	MPMLQ	6.3	16	30	30	3.9
G.723.1	ACELP	5.3	16	30	30	3.6

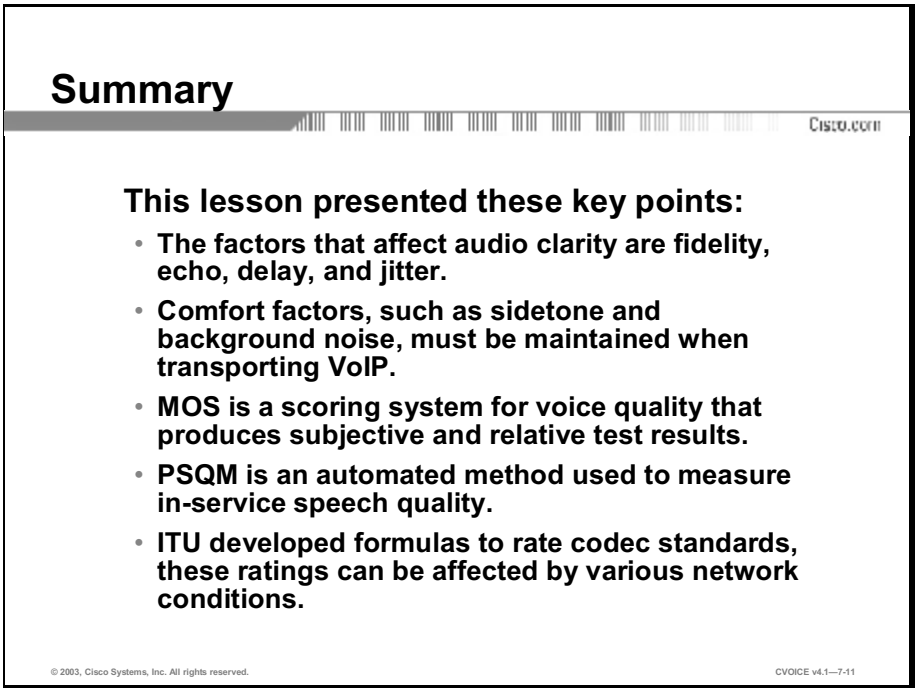
The International Telecommunications Union (ITU) conducted MOS testing to develop formulas for rating standards G.711 through G.729. The results are summarized in the table here.



This figure demonstrates how the MOS rating for the coder-decoder (codec) quality score G.729 is affected by various network conditions.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Voice Quality Measurement
- VoIP Challenges lesson

Quiz: Voice Quality Measurement

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- List the attributes that affect audio clarity
- Describe the psychological comfort factors that affect voice quality
- State the purpose of mean opinion score and the method used to calculate it
- State the purpose of Perceptual Speech Quality Measurement and the method used to calculate it
- Describe how the voice quality score differences between various coder-decoder examples are measured

Instructions

Answer these questions:

Q1) Which two factors contribute to delay variation in voice transmission? (Choose two.)

A) congestion on the network

B) electrical impedance mismatches

C) compression of packets

D) inconsistency in bandwidth

E) varying routes of packets

Q2) Which two factors affect voice clarity? (Choose two.)

A) fidelity

B) echo

C) sidetone

D) background noise

E) distance

Q3) Which two 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

Q4) What is the disadvantage of using VAD on a call?

A) The cost of the call may increase.

B) The listener may hear unwanted noise.

C) The bandwidth requirement may increase.

D) The speaker may think that the connection is broken.

Q5) Which voice quality scoring system is based on subjective evaluation?

A) MOS

B) PCM

C) PSQM

D) YBTM

Q6) Why is it important to establish a baseline when using MOS for evaluating voice quality?

A) The results are linear.

B) The results are relative.

C) The results are compiled infrequently.

D) The results are too hard to interpret.

Q7) How is PSQM measured?

A) by comparing original speech with transmitted speech

B) by having listeners score transmitted speech

C) by having listeners score prerecorded sentences

D) by using Cisco equipment and software for measuring transmitted speech

Q8) 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

Q9) Which codec scores highest in MOS testing?

A) G.711

B) G.723.1

C) G.726

D) G.728

E) G.729

Q10) According to MOS tests, which network condition distorts voice the least?

A) 5 percent bit error rate

B) 5 percent frame error rate

C) two tandem codings

D) three tandem codings

E) low input level

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

VoIP Challenges

Overview

Because of the inherent characteristics of a converged voice and data IP network, administrators face certain challenges in delivering voice traffic correctly. This section lists and describes these challenges and offers solutions to avoid and overcome them.

Importance

Administrators of converged networks must consider and overcome technical challenges that hinder the proper delivery of voice packets. Network administrators must complete and understand this lesson before they can successfully implement a converged voice and data IP network.

Objectives

Upon completing this lesson, you will be able to:

- Name some of the inherent problems that occur when delivering voice in IP networks
- Describe the cause of jitter and the solution that is used to eliminate jitter from an IP network
- List the two types of packet delay and the solution that is used to eliminate packet delay from an IP network
- State the cause and effect of packet loss on voice quality
- Describe the contention issues associated with transmitting voice and data on the same outbound interface
- Describe the methods that are used to sequence voice packets
- Describe the effect of circuit reliability and availability on voice quality

Learner Skills and Knowledge

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

- Knowledge of Voice over IP (VoIP) basics
- Knowledge of TCP/IP networks including routing, User Datagram Protocol (UDP), and best-effort concepts
- Knowledge of traditional telephony networks

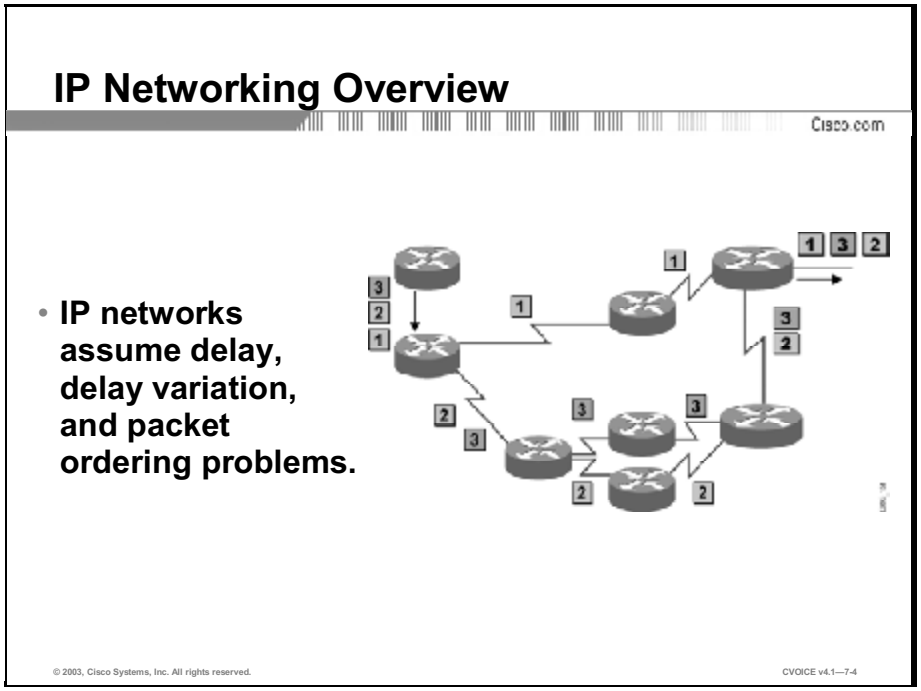
Outline

This lesson includes these topics:

- Overview
- IP Networking Overview
- Jitter
- Delay
- Effect of Packet Loss on Quality
- Competition Between Voice and Data for Bandwidth
- Packet Sequencing
- Reliability and Availability
- Summary
- Assessment (Quiz): VoIP Challenges

IP Networking Overview

This topic provides an overview of IP networking and some of the inherent challenges when conveying voice over an IP network.



IP is a connectionless network protocol. Connectionless networks generally do not participate in signaling. The concept of session establishment exists between end systems, although the connectionless network remains unaware of the virtual circuit (VC).

IP resides at the network layer of the Open System Interconnection (OSI) protocol stack. Therefore, it can transport IP packets over deterministic and nondeterministic Layer 2 protocols, such as Frame Relay or ATM. IP can be used to communicate across any set of interconnected networks and is equally suited to both LAN and WAN communication.

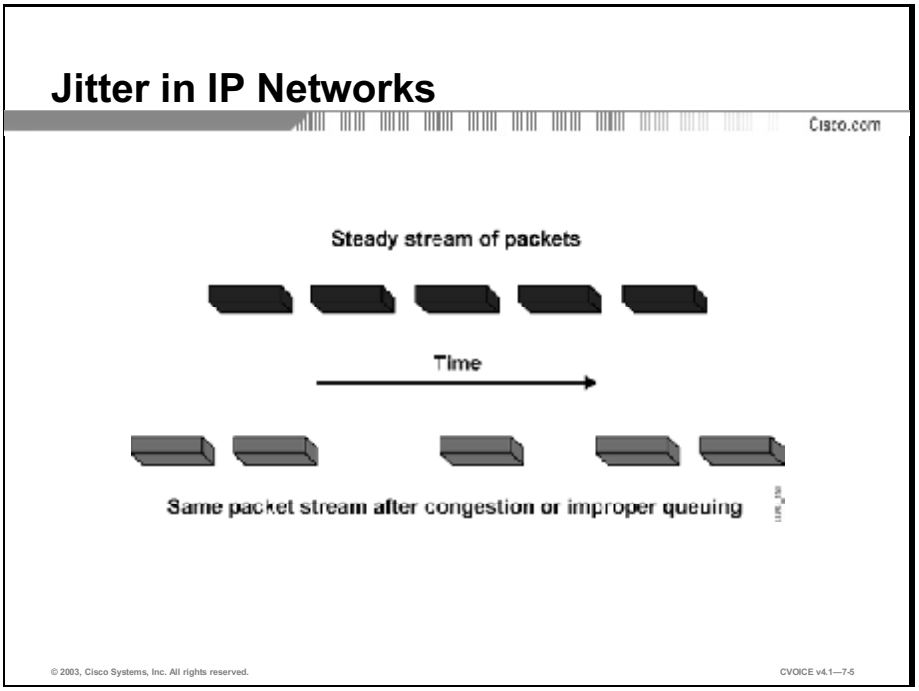
IP information is transferred in a sequence of datagrams. A message is sent as a series of datagrams that are reassembled into the completed message at the receiving location. Because a voice conversation that is transported in IP can be considered a continuous audio file, all packets must be received in sequence immediately and without interpacket variable delay.

Traditionally, IP traffic transmits on a FIFO basis. Different packet types vary in size, allowing large file transfers to take advantage of the efficiency that is associated with larger packet sizes. FIFO queuing affects the way that voice packets transmit, causing delay and delay variation at the receiving end.

The User Datagram Protocol (UDP) is the connectionless transport layer protocol used for Voice over IP (VoIP). UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery. UDP requires that other protocols handle error processing and retransmission. The figure shows how packets may be received out of sequence, or completely lost at the receiving end.

Jitter

This topic describes the occurrence of jitter in IP networks and the Cisco Systems solution to this problem.

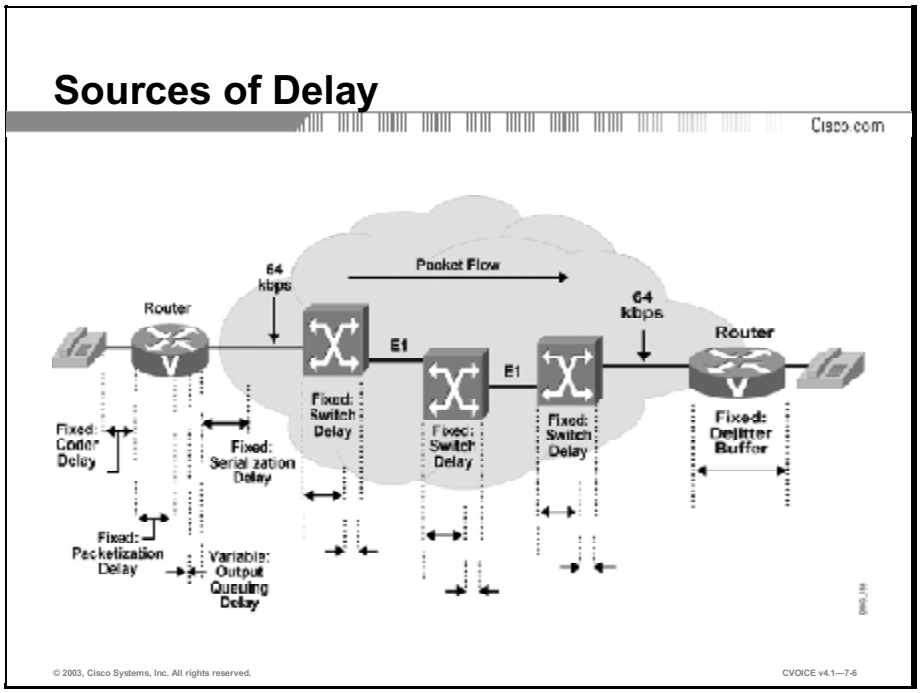


Jitter is defined as a variation in the delay of received packets. On the sending side, packets are sent in a continuous stream with the packets spaced evenly apart. Because of network congestion, improper queuing, or configuration errors, this steady stream can become lumpy, or the delay between each packet can vary 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. 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 is also referred to as the *dejitter buffer*. The playout delay buffer, however, affects overall absolute delay.

Delay

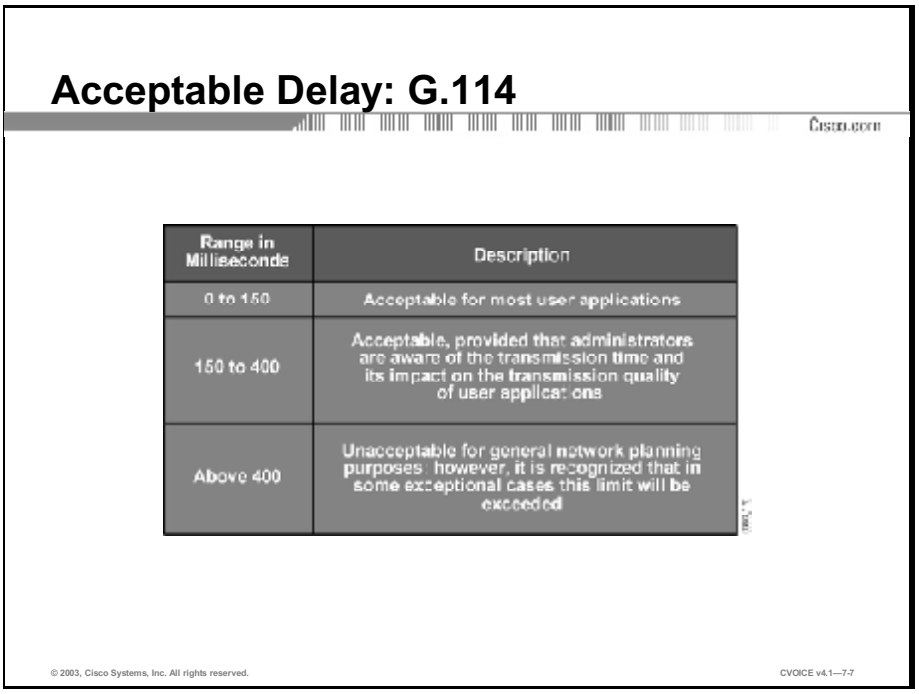
Overall or absolute delay can affect VoIP. You might have experienced delay in a telephone conversation with someone on a different continent. The delays can be very frustrating, causing words in the conversation to be cut off. This topic describes the causes of packet delay and the Cisco solution to 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 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.

There are two distinct types of delay:

- Fixed-delay components add directly to the overall delay on the connection.
- 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.



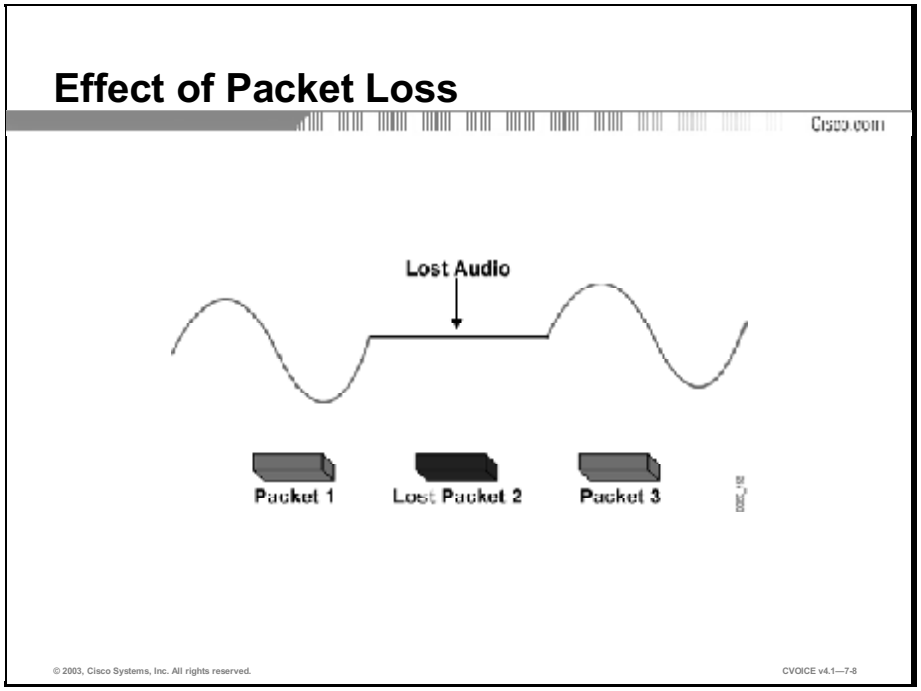
The International Telecommunication Union (ITU) considers network delay for voice applications in Recommendation G.114. This recommendation defines three bands of one-way delay, as shown in the table in the figure.

Note	These recommendations are for connections with echo that are adequately controlled; this implies that echo cancellers are used. Echo cancellers are required when one-way delay exceeds 25 ms (G.131).

These recommendations are oriented toward national telecom administrations, and therefore they are more stringent than the 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. However, all networks must be engineered so that the maximum expected voice connection delay is known and minimized.

Effect of Packet Loss on Quality

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.



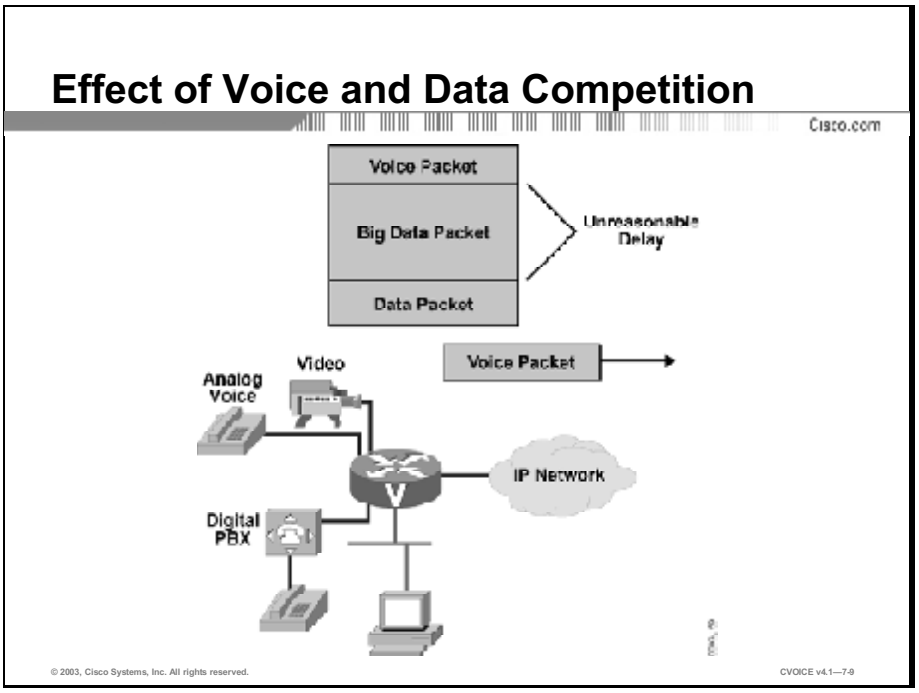
Voice packets might be dropped under the following conditions:

- The network quality is poor
- The network is congested
- There is too much variable delay in the network

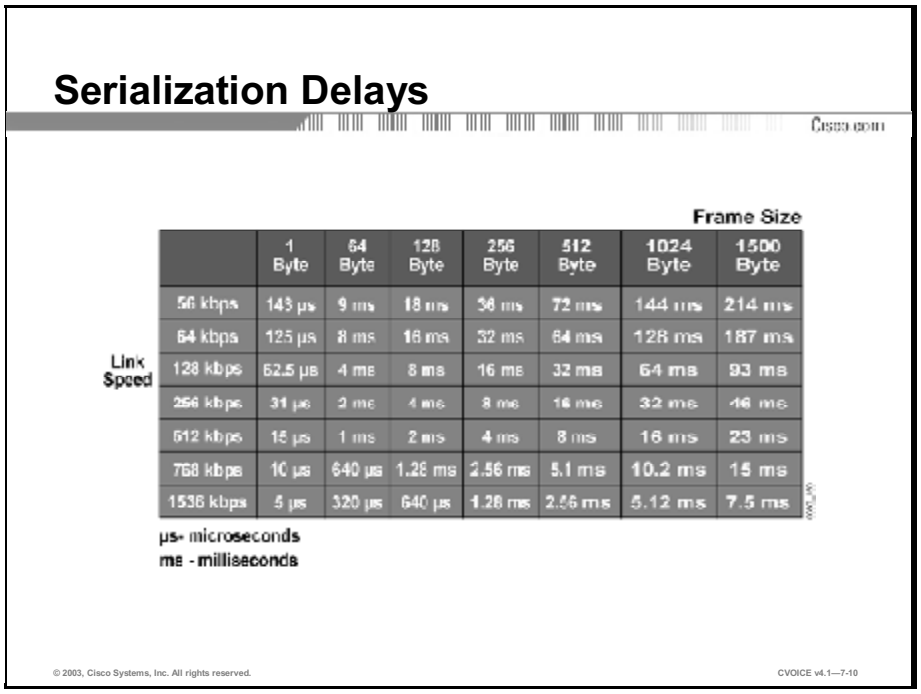
Packet loss causes voice clipping and skips; as a result, the listener hears gaps in the conversation, as shown in the figure. The industry standard coder-decoder (codec) algorithms that are used in Cisco DSPs will correct for 20 to 50 ms of lost voice. Cisco VoIP technology uses 20 ms samples of voice 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 are lost, the listener experiences gaps.

Competition Between Voice and Data for Bandwidth

In a converged network, voice and data packets compete with each other for transmission on the outbound interface. This topic describes the effects of this competition and offers solutions.



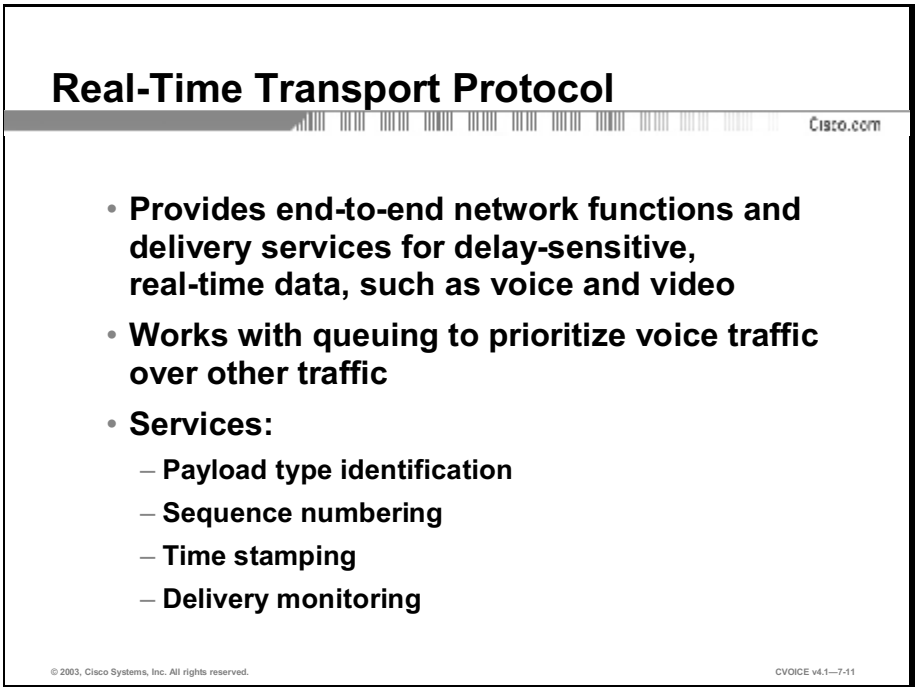
When both data and voice are placed in the same output queue, voice can suffer delay and delay variation. The time it takes to transmit large data packets can cause voice problems that result in communication gaps.



This table in the figure shows the delay problems that occur when dealing with large packets and slow links. When you are calculating acceptable delay, slower links may require that you fragment larger packets and prioritize voice packets.

Packet Sequencing

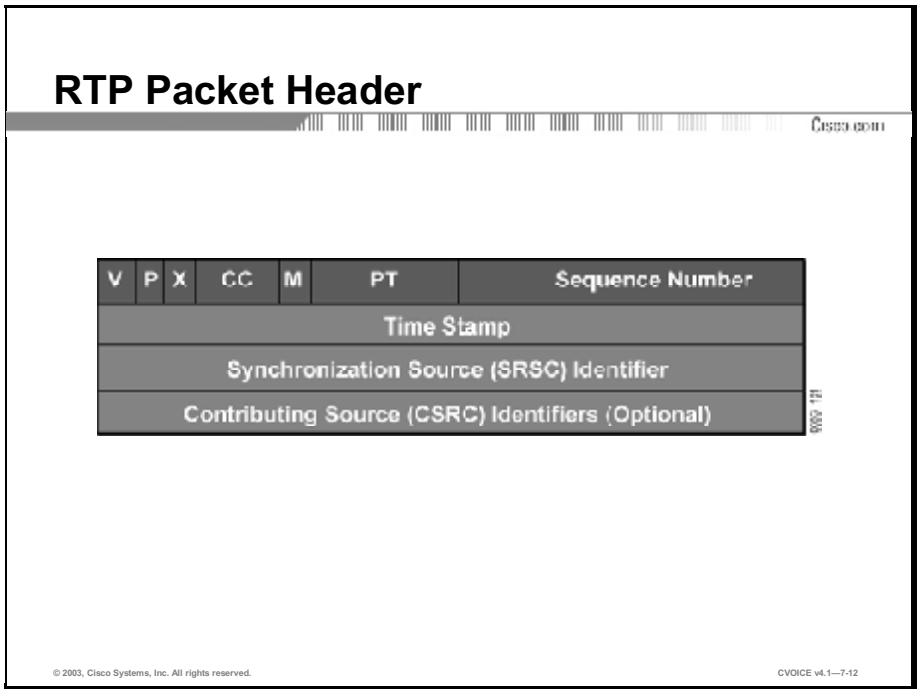
Because voice packets are carried using UDP over IP, packets often arrive out of sequence at the receiving end. This topic describes the method that you must use to sequence packets.



Real-Time Transport Protocol (RTP) provides end-to-end network functions and delivery services for delay-sensitive, real-time data, such as voice and video.

To support VoIP, RTP works with queuing to prioritize voice traffic over other traffic. RTP services include the following:

- Payload-type identification
- Sequence numbering
- Time stamping
- Delivery monitoring



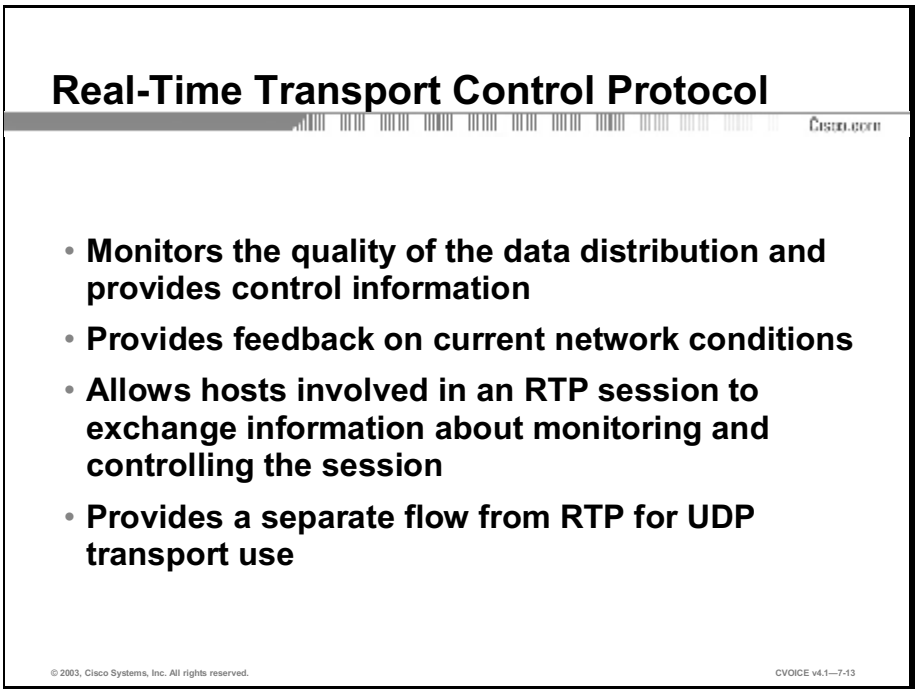
The RTP header consists of nine fields and is a minimum of 12 bytes. If multiple sources are included in the stream, the optional contributing source identifier field (CSRC) contents are appended to the end of the RTP header.

The table shows the RTP fields, their lengths and their uses.

Table 1: RTP

Field	Length	Use
Version (V)	2 bits	RTP version; current version is 2
Padding (P)	1 bit	Indicates if the header has padding bits at the end
Extension (X)	1 bit	If set, indicates that exactly one header extension is included
Contributing source count (CC)	4 bits	Number of CSRC identifiers in the CSRC field following the initial RTP header
Marker (M)	1 bit	Interpretation defined by a profile
Payload type (PT)	7 bits	Payload type, frequently the codec type
Sequence	16 bits	Sequential number, beginning with a random number, that the receiver may use to indicate packet loss
Time stamp	32 bits	Time stamp of the first octet of data in the RTP data packet; the initial value is a random value
Synchronization source (SRSC)	32 bits	Randomly chosen value used within a data stream to permit multiplexing multiple streams
Contributing source (CSRC)	0 to 15 items, 32 bits each	If multiple streams are mixed into a single stream, the list of source streams is included here; for example, in a conference where multiple streams are sent, each participant is marked as a separate contributing source

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



RTP Control Protocol (RTCP) monitors the quality of the data distribution and provides control information. It provides the following feedback on current network conditions:

- A mechanism for hosts involved in an RTP session to exchange information about monitoring and controlling the session. RTCP monitors quality for such elements as packet counts, packets lost, and interarrival jitter. RTCP generally allocates a fixed 5 percent of total session bandwidth (for its own use) with a minimum interval of 5 seconds between RTCP packets. RTCP imposes these limits on itself so that is does not interfere with the packets that carry the digitized voice.

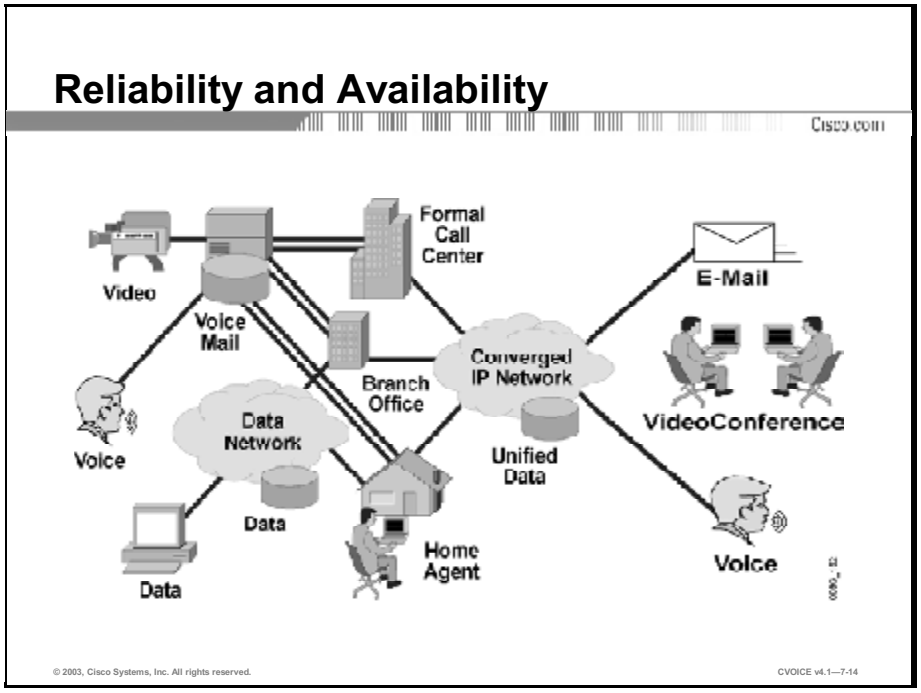
- A separate flow from RTP for UDP transport use.

Both RTP and RTCP are detailed in the H.323 specification. After the H.323 call setup and control process is complete, UDP sends audio and video packets. You must remember that UDP cannot guarantee packet delivery and ordering. To assist with streaming audio and video, the H.323 specification calls for an RTP header.

An RTP header contains a time stamp and sequence number that enables the receiving device to buffer as much as necessary to remove jitter and latency by synchronizing the packets to play back a continuous stream of sound.

Reliability and Availability

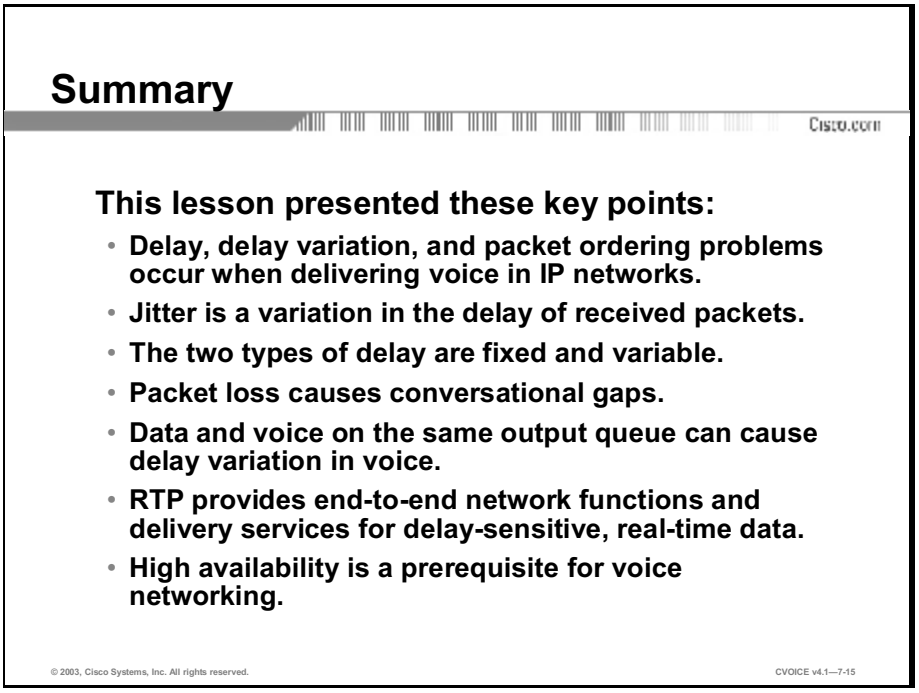
This topic discusses the importance of reliability and availability of the converged network.



A prerequisite for voice networking is high availability as shown in the figure. Voice networks are often considered more critical and available than their data-centric counterparts. This situation exists even though e-mail is considered the primary form of business communications media and is more popular than voice. Therefore, the availability and reliability of the data network is every bit as important as the voice network. Cisco Architecture for Voice, Video and Integrated Data (AVVID) is a distributed architecture that is inherently available and scalable. The ability to seamlessly provide additional capacity for infrastructure, services, and applications is a unique benefit of the architecture. Cisco CallManager clusters can scale to thousands of users. This technology is highly dependable and is used in Cisco business operations.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): VoIP Challenges
- Quality of Service and Good Design lesson

References

For additional information, refer to these resources:

- "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
- "QoS Documentation" http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/avvidqos/qosintro.htm

Quiz: VoIP Challenges

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Name some of the inherent problems that occur when delivering voice in IP networks
- Describe the cause of jitter and the solution that is used to eliminate jitter from an IP network
- List the two types of packet delay and the solution that is used to eliminate packet delay from an IP network
- State the cause and effect of packet loss on voice quality
- Describe the contention issues associated with transmitting voice and data on the same outbound interface
- Describe the method that is used to sequence voice packets
- Describe the effect of circuit reliability and availability on voice quality

Instructions

Answer these questions:

Q1) Which feature of an IP network causes delay and delay variation in voice traffic?

A) connectionless transmission

B) fragmentation and reassembly

C) FIFO queuing

D) no error correction or acknowledgements

Q2) Which Layer 4 protocol is used for transmitting packets in VoIP networks?

A) IP

B) TCP

C) UDP

D) Frame Relay

Q3) How can you 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) According to ITU-T Recommendation G.114 for national telecom administrations, how much delay is acceptable for most user applications?

A) 0 to 150 ms

B) 200 to 250 ms

C) 150 to 400 ms

D) above 400 ms

Q6) According to Cisco, what is the acceptable level of one-way delay for private networks?

A) 0 to 150 ms

B) 200 to 250 ms

C) 150 to 400 ms

D) above 400 ms

Q7) 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

Q8) Which conditions can result in voice packets being dropped?

A) slow links

B) too much noise

C) too much jitter

D) none of the above

Q9) What is the major cause of delay when voice and data packets are placed in the same output queue?

A) large packets

B) low bandwidth

C) firewalls

D) retransmission of lost packets

Q10) What two techniques can be used on slower links in a voice and data network to reduce delay in voice transmission? (Choose two.)

A) FIFO queuing

B) buffering of voice packets

C) fragmentation of large packets

D) prioritization of voice packets

E) compression of packets

Q11) What is the size of the RTP header?

A) 3 bytes

B) 5 bytes

C) 12 bytes

D) 40 bytes

Q12) Which RTP header field is used to allow multiplexing of multiple data streams?

A) contributing source count

B) marker

C) payload type

D) sequence

E) time stamp

F) synchronization source

G) contributing source

Q13) What is one of the main benefits of using Cisco AVVID for voice and data networks?

A) seamless scalability of infrastructure and applications

B) ability to provide equal quality for voice and data

C) low cost of implementation

D) integration with legacy networks

Q14) Which factor is a prerequisite for voice networking?

A) TCP sessions

B) FIFO queuing

C) high availability

D) low cost

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Quality of Service and Good Design

Overview

This lesson introduces the concept of quality of service (QoS) as it applies to a converged network and guides the student through resources to learn more about QoS.

Importance

Successful implementation of Voice over IP (VoIP) requires an overall understanding of QoS and knowledge of QoS resources.

Objectives

Upon completing this lesson, you will be able to:

- Describe the problems that are associated with transmitting voice in converged networks
- List five ways that QoS improves voice quality
- Identify the features that are offered by Cisco IOS QoS for voice at different points in the network
- Describe two certification courses that are offered by Cisco as resources for network administrators
- Find information about QoS in the appropriate location on the Cisco.com website
- List three Cisco Press publications that can be used as resources for network administrators

- Identify four characteristics of a poorly designed VoIP network
- List the Cisco educational resources that are available for QoS implementation methods

Learner Skills and Knowledge

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

- Knowledge of VoIP networks
- Knowledge of traditional telephony networks
- Knowledge of TCP/IP networks

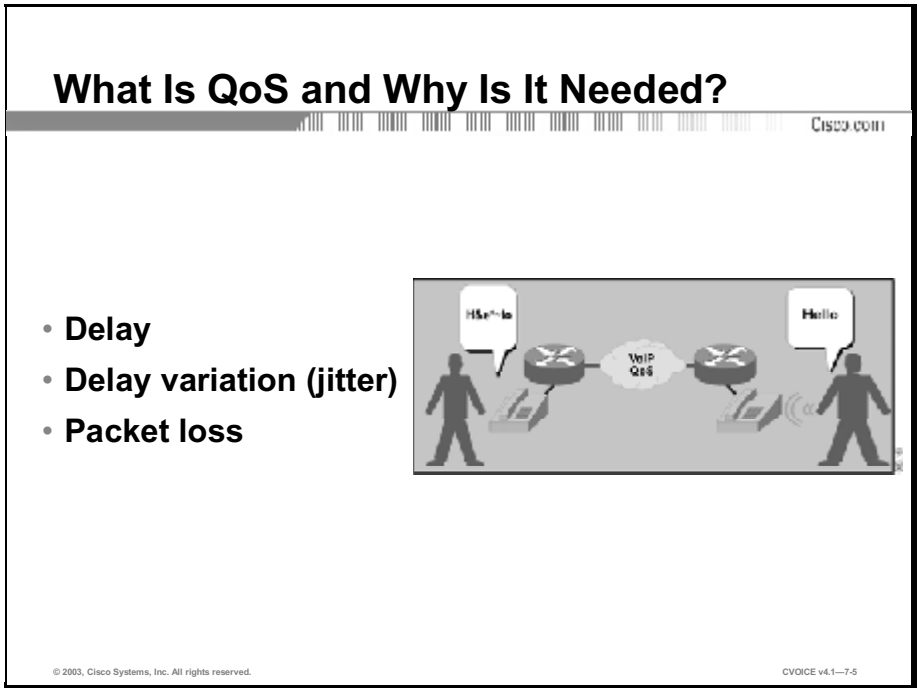
Outline

This lesson includes these topics:

- Overview
- Need for QoS Mechanisms
- Objectives of QoS
- Applying QoS for End-to-End Improvement of Voice Quality
- Cisco Certified Training Courses
- Cisco.com
- Cisco Press Publications
- Characteristics of Bad Design
- Resources for Design Practices
- Summary
- Assessment (Quiz): Quality of Service and Good Design

Need for QoS Mechanisms

This topic lists the problems that are associated with transmitting voice over a data network.

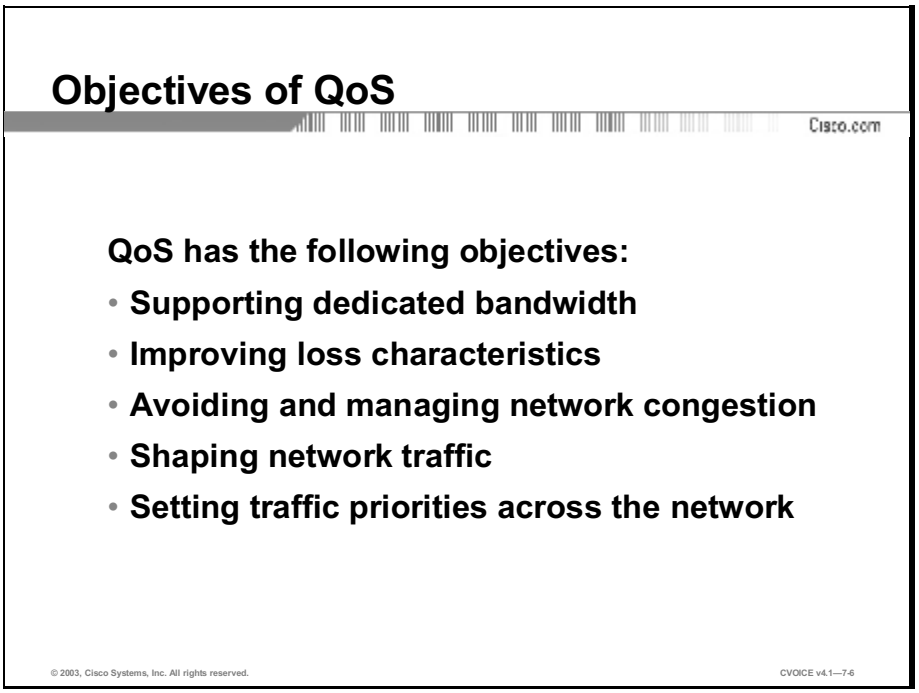


Real-time applications, such as voice applications, have different characteristics and requirements than traditional data applications. Voice applications tolerate minimal variation in the amount of delay. This affects delivery of voice packets. Packet loss and jitter degrade the quality of the voice transmission that is delivered to the recipient. The figure shows how these problems can affect a voice message.

To effectively transport voice traffic over IP, you must have mechanisms that ensure the reliable delivery of packets with low latency. Cisco IOS® features have the mechanisms for meeting voice packet delivery requirements.

Objectives of QoS

To ensure that Voice over IP (VoIP) is a realistic 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 quality of service (QoS) can you help achieve this objective.



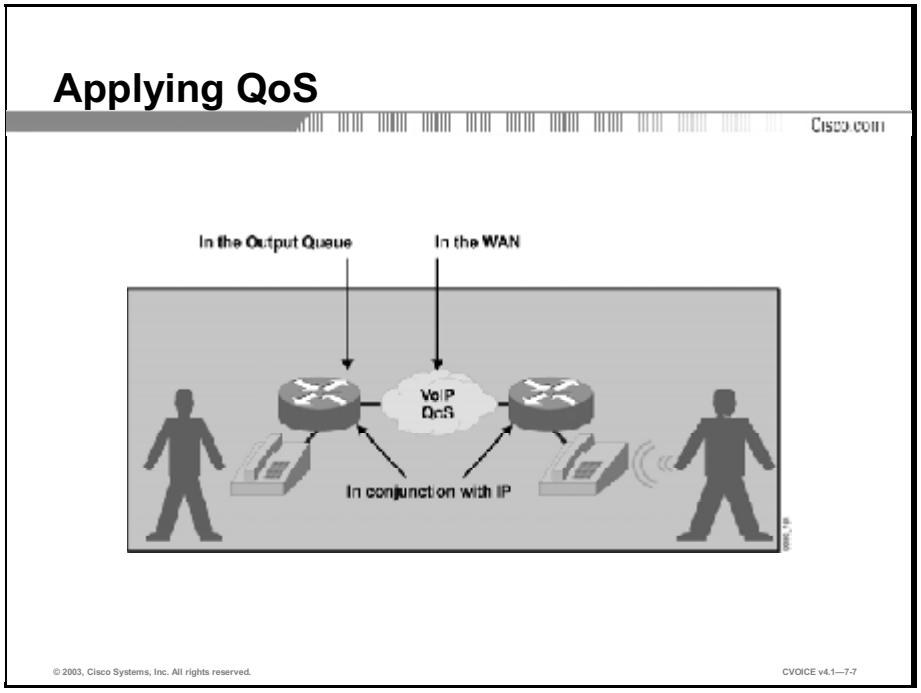
Like other real-time applications, VoIP is extremely sensitive to issues related to bandwidth and delay. To ensure that VoIP transmissions are intelligible to the receiver, voice packets cannot be dropped, excessively delayed, or subject to variations in delay (also known as jitter).

VoIP guarantees high-quality voice transmission only if the signaling and audio channel packets have priority over other kinds of network traffic. To deploy VoIP, you 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 performing the following:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

Applying QoS for End-to-End Improvement of Voice Quality

Voice features for Cisco IOS QoS are deployed at different points in the network and designed for use with other QoS features to achieve specific goals; for example, control over jitter and delay. This topic lists the network areas where Cisco IOS QoS is implemented.



Cisco IOS software includes a complete set of features for delivering QoS throughout the network. Following are 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):** 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):** Provides strict priority queuing on ATM virtual circuits (VCs) and serial interfaces. LLQ configures the priority status for a class within CBWFQ and is not limited to User Datagram Protocol (UDP) port numbers (as in IP RTP Priority). LLQ is considered a “best practice” by the Cisco Enterprise Solutions Engineering (ESE) group for delivering voice QoS services over a WAN.
  - **WFQ and Distributed WFQ (DWFQ):** Segregates traffic into flows and then schedules traffic onto the outputs to meet specified bandwidth allocation or delay bounds.

- **Weighted Random Early Detection (WRED) and Distributed WRED (DWRED):** 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):** Provides a rate-limiting feature for allocating bandwidth commitments and bandwidth limitations to traffic sources and destinations. At the same time, it specifies policies for handling the traffic that may exceed bandwidth allocation.

  - **Frame Relay traffic shaping (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.

  - **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 VC with fragments of a long frame on another VC that is using the same interface.

  - **IP to ATM class of service (CoS):** Includes a feature suite that maps CoS characteristics between the IP and ATM. It also offers differential 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):** Allows large packets to be multilink-encapsulated and fragmented so that they are small enough to satisfy the delay requirements of real-time traffic. 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 IP operation:
  - **Compressed Real-Time Transport Protocol (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):** 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):** Steadies 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.

Cisco Certified Training Courses

A number of resources are available to help network administrators understand and implement QoS. This topic describes two certification courses that Cisco offers.

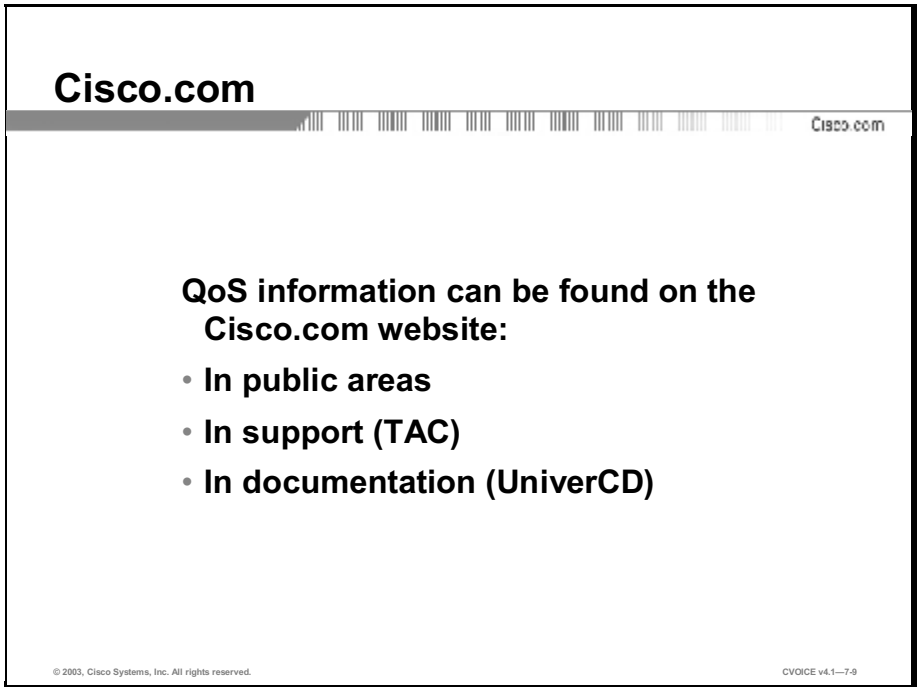
Cisco Systems offers the following two certification courses:

- **"Deploying Cisco QoS for Enterprise Networks" (DQoS):** This course provides system engineers and network engineers the knowledge and skills required to deploy, manage, configure, and troubleshoot QoS features available through Cisco IOS Release 12.1(5)T. The focus is on tuning the enterprise network with QoS tools that enable high profile, mission-critical traffic to perform at an optimal level.

- **"Implementing Cisco Quality of Service" (IQoS):** This course describes the need for QoS mechanisms in IP networks. It describes the two conceptual QoS models (Integrated Services and Differentiated Services [DiffServ]), basic technologies, classification and marking, queuing mechanisms, traffic shaping and policing, congestion avoidance, link efficiency, signaling mechanisms, Modular QoS Command Line Interface (MQC), and IP over ATM.

Cisco.com

The Cisco.com website is a resource that provides network administrators with additional information on QoS. This topic lists the QoS resources.



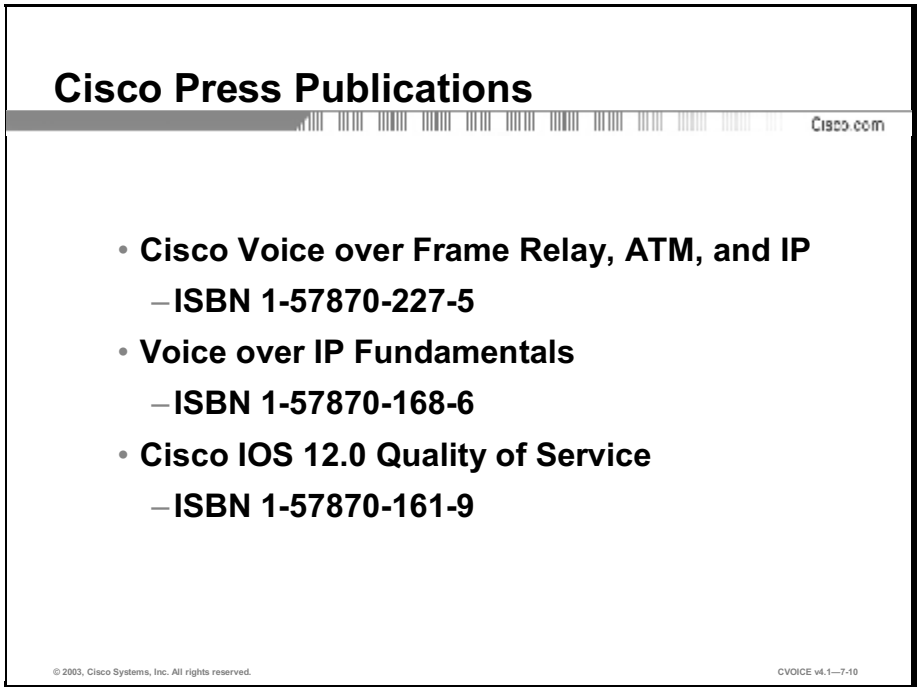
Information about QoS on the Cisco.com website is found:

- **In public areas:**
  - Voice Quality (Quality of Service)
    http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Technologies&f=1533
  - Graphical Navigation Guide for VoIP Issues
    http://www.cisco.com/warp/public/788/voip/voice-ms-nav-guide-1.html
  - Understanding Delays in Packet Voice Networks
    http://www.cisco.com/warp/public/788/voip/delay-details.html
  - Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)
    http://www.cisco.com/warp/public/788/voice-qos/jitter_packet_voice.html
- **In support:**
  - Technical Support: Voice Quality
    http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:Voice:QoS

- **In documentation (UniverCD):**
  - Congestion Management Overview
    http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt2/qcfconmg.htm#48685

Cisco Press Publications

This topic lists Cisco Press publications that can be helpful to network administrators in understanding and implementing QoS.

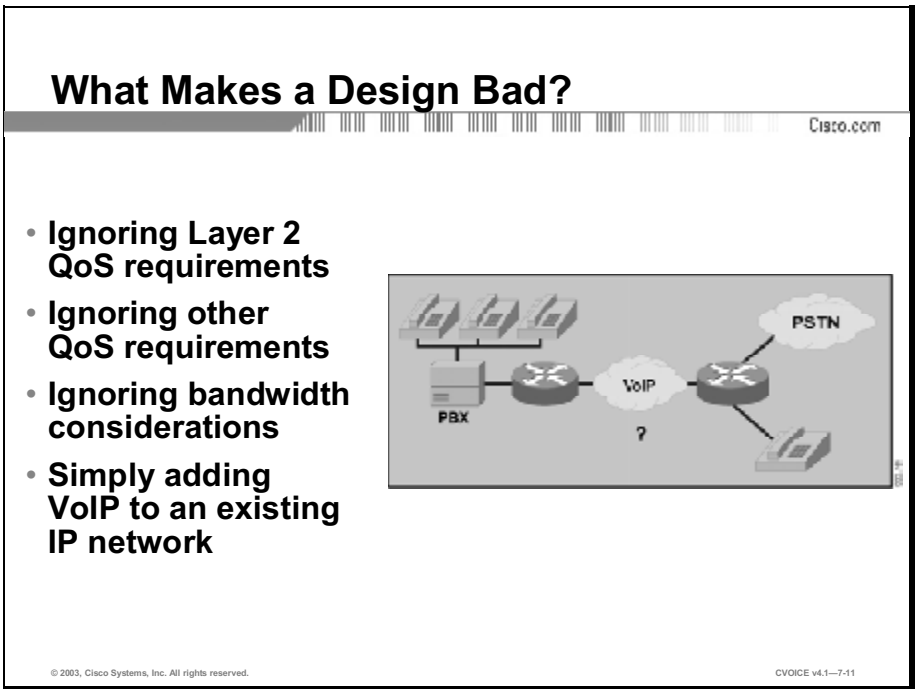


Cisco Press publications are also excellent sources of information. The following titles may be helpful:

- *Cisco Voice over Frame Relay, ATM, and IP*
  - ISBN 1-57870-227-5
- *Voice over IP Fundamentals*
  - ISBN 1-57870-168-6
- *Cisco IOS 12.0 Quality of Service*
  - ISBN 1-57870-161-9

Characteristics of Bad Design

A network that is well-engineered from end to end is necessary for running delay-sensitive applications such as VoIP. Fine-tuning the network to adequately support VoIP involves a series of protocols and features that are geared toward improving QoS. This topic identifies characteristics of a poorly designed network.



QoS is the ability of a network to provide DiffServ 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.

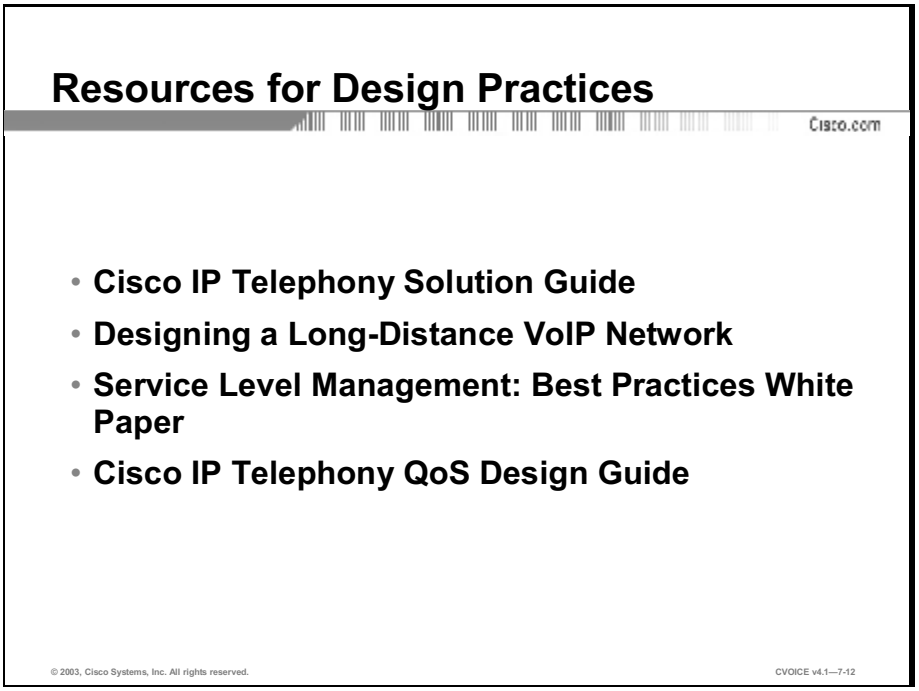
Poor design characteristics include:

- **Ignoring Layer 2 QoS requirements:** Layer 2 QoS includes FRF.11, LFI , and traffic shaping.
- **Ignoring other QoS requirements:** Services, such as LLQ and RTP 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.

You must configure QoS throughout the network—not simply on the Cisco devices that are running VoIP—to improve voice network performance. 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 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 then select the appropriate QoS tools.

Resources for Design Practices

Well-designed networks usually come at the expense of trial and error. This topic lists various resources that Cisco offers to help you design a voice network that operates optimally.



Many resources are available through the Cisco.com website. You can access these resources by using the search tool on the main page. Here are two examples:

- To help organizations prepare for Cisco IP telephony, Cisco offers the *Cisco IP Telephony Solution Guide*, and the Web-based *Cisco IP Telephony Readiness Assessment*. These resources help organizations implement both the network design needed to support IP telephony and the Cisco IP telephony solution itself.
  - IP Telephony Readiness Assessment (A user ID and password are required to access this site.) http://tools.cisco.com/Assessments/jsp/welcome.jsp?asmt=VOIP
- The long-distance VoIP network design solution includes multiple components in various combinations from both Cisco and third-party vendors. Voice points of presence (POPs) connected to other service providers are a central component in the delivery of wholesale voice services. The types of interconnections, or call topologies, that service providers support will determine the specific components and design methods that Cisco recommends.
  - Designing a Long-Distance VoIP Network http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/longd.htm

- A white paper that describes service level management and service level agreements (SLAs) can be found on the Cisco website:

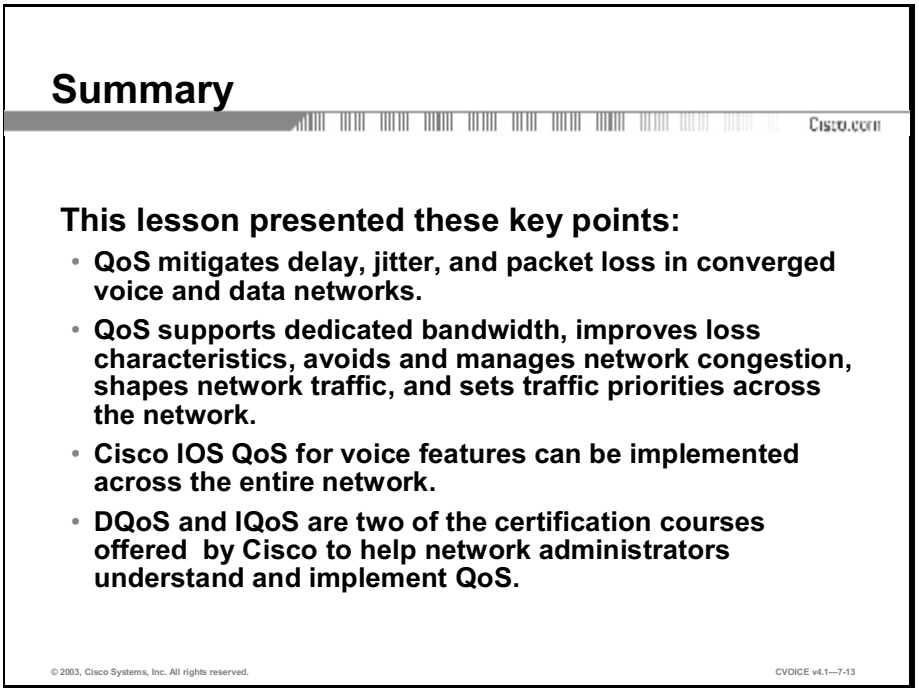
  – Service Level Management: Best Practices White Paper
  http://www.cisco.com/warp/public/126/sla.htm

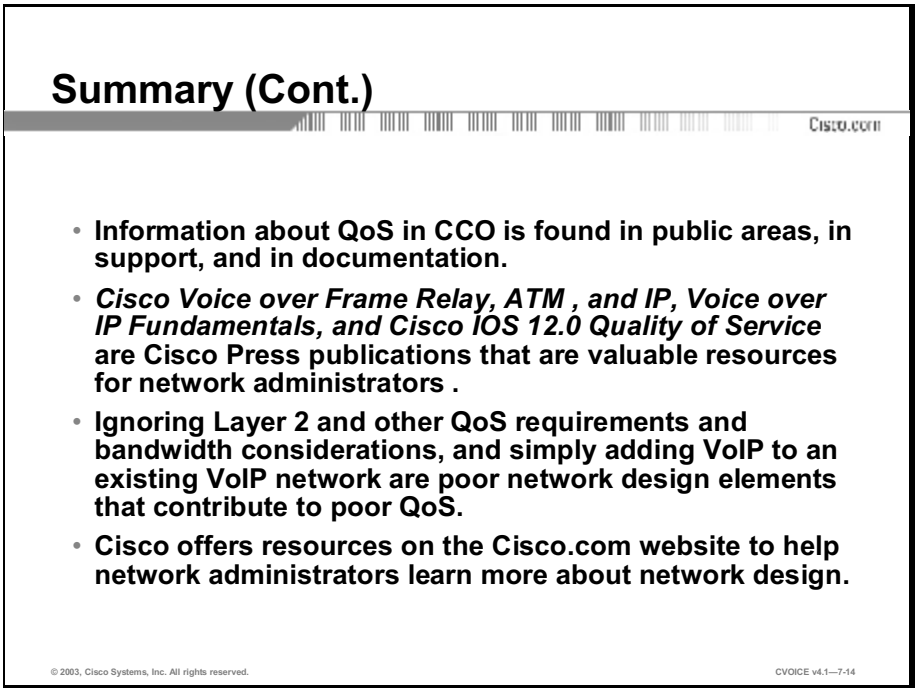
- To help organizations plan for and implement QoS, *Cisco IP Telephony QoS Design Guide* suggests strategies for both campus and WAN environments. This information can be found on the Cisco website:

  – Cisco IP Telephony Network Design Guides
  http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/iptlink.htm

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Quality of Service and Good Design
- Understanding Jitter lesson

References

For additional information, refer to these resources:

- "Voice Quality"
  http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:Voice:QoS
- "Voice Quality (Quality of Service)"
  http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Technologies&f=1533

Quiz: Quality of Service and Good Design

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the problems that are associated with transmitting voice in converged networks
- List five ways that QoS improves voice quality
- Identify the features that are offered by Cisco IOS QoS for voice at different points in the network
- Describe two certification courses that are offered by Cisco as resources for network administrators
- Find information about QoS in the appropriate location on the Cisco.com website
- List three Cisco Press publications that can be used as resources for network administrators
- Identify four characteristics of a poorly designed VoIP network
- List the Cisco educational resources that are available for QoS implementation methods

Instructions

Answer these questions:

Q1) Which two factors have a minimal effect on data transmissions but negatively impact voice transmissions? (Choose two.)

A) high bandwidth

B) T1 links

C) packet loss

D) jitter

E) Layer 2 protocol

Q2) What are the two requirements of effective voice transmission over an IP network? (Choose two.)

A) low latency

B) G.711 codecs

C) reliable delivery of packets

D) use of compression algorithms

E) high-speed links

Q3) 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

Q4) 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

Q5) Which two Cisco IOS 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

Q6) 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

Q7) If you want to learn about troubleshooting QoS features provided by Cisco IOS Release 12.1(5)T, which certification course should you take?

A) Deploying Cisco QoS for Enterprise Networks

B) Implementing Cisco Quality of Service

C) Cisco IOS 12.0 Quality of Service

D) Cisco IP Telephony Network Design

Q8) Which Cisco course describes the Integrated Services and the Differentiated Services QoS models?

A) Service Level Management

B) Cisco IP Telephony Network Design

C) Deploying Cisco QoS for Enterprise Networks

D) Implementing Cisco Quality of Service

Q9) Which three areas of the Cisco.com website contain information about QoS? (Choose three.)

A) documentation

B) private

C) products

D) public

E) publications

F) support

Q10) In which area of Cisco.com would you find the document “Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)”?

A) public

B) support

C) documentation

Q11) Which title is a Cisco Press publication that may be helpful for understanding QoS implementation?

A) Cisco IP Telephony Solution Guide

B) Designing a Long Distance VoIP Network

C) Cisco IOS 12.0 Quality of Service

D) Graphical Navigation Guide for VoIP Issues

Q12) Which title is published by Cisco Press to help network administrators understand and implement QoS?

A) Cisco IP Telephony Network Design Guide

B) IP Telephony Readiness Assessment

C) Voice over IP Fundamentals

D) Voice Quality (Quality of Service)

Q13) Which practice indicates a bad network design?

A) completely redesigning the network

B) using low latency queuing

C) ignoring Layer 3 QoS requirements

D) ignoring bandwidth requirements

Q14) 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

Q15) Which resource on Cisco.com provides information on the specific components and design methods recommended by Cisco for long-distance VoIP networks?

A) Cisco IP Telephony Network Design Guide

B) IP Telephony Readiness Assessment

C) Voice over IP Fundamentals

D) Deploying Cisco QoS for Enterprise Networks

E) Designing a Long-Distance Telephone Network

Q16) Which resource on Cisco.com is meant to help organizations plan for and implement QoS?

A) Implementing Cisco Quality of Service

B) Cisco IP Telephony Network Design Guides

C) Service Level Management: Best Practices White Paper

D) Designing a Long-Distance Telephone Network

E) Deploying Cisco QoS for Enterprise Networks

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Understanding Jitter

Overview

This topic describes jitter and the methods that are used to measure and compensate for it.

Importance

Jitter and its effects can cause significant distortions in Voice over IP (VoIP). Network administrators must be aware of the causes of and solutions for jitter phenomena in VoIP networks.

Objectives

Upon completing this lesson, you will be able to:

- Explain the reasons for jitter in a converged network and list two ways that networks can compensate for it
- Describe the methods that are used on Cisco Systems voice routers to overcome the problem of jitter
- Identify three symptoms that require the adjustment of playout delay buffer parameters
- Describe all the fields in the **show call active voice** command output that indicate the size of jitter
- Use the **playout-delay mode adaptive** command to configure a dynamic jitter buffer mode
- Use the **playout-delay mode fixed** command to configure a static jitter buffer mode

Learner Skills and Knowledge

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

- Knowledge of traditional telephony
- Knowledge of VoIP basics
- Knowledge of TCP/IP networks

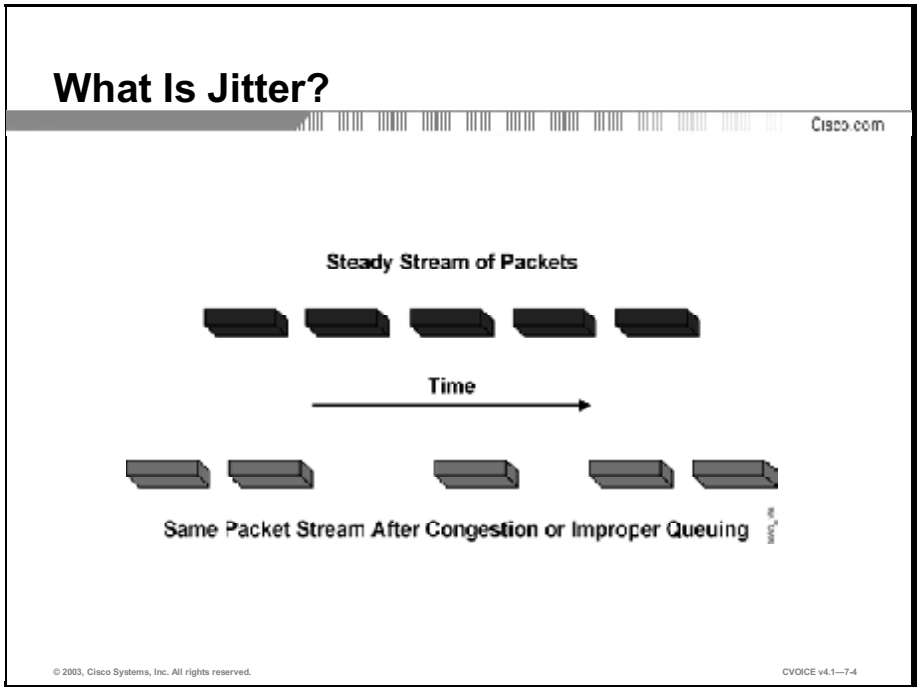
Outline

This lesson includes these topics:

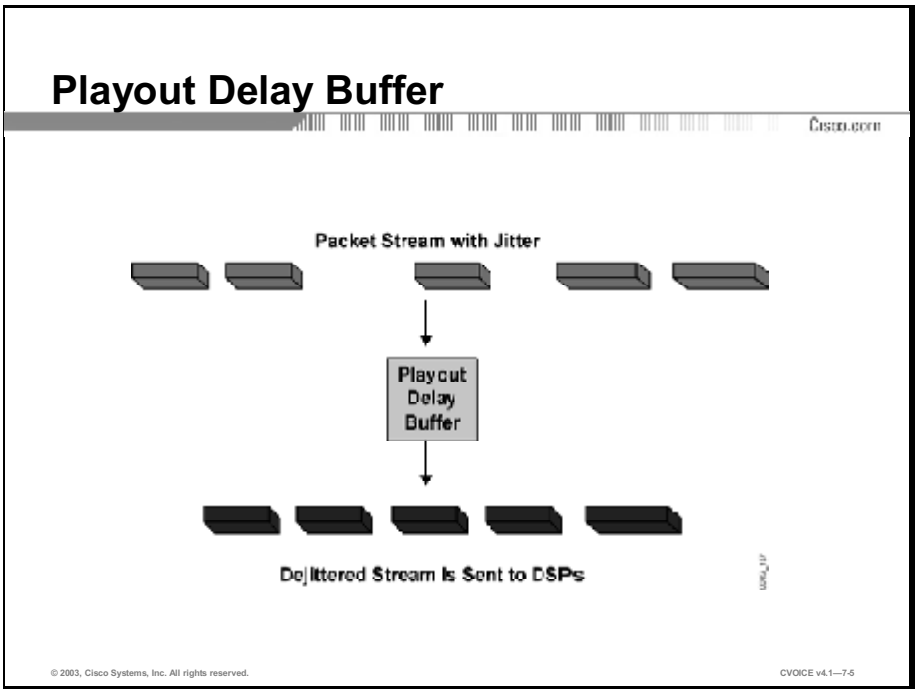
- Overview
- Understanding Jitter
- Overcoming Jitter
- Adjusting Playout Delay Parameters
- Symptoms of Jitter on a Network
- Dynamic Jitter Buffer
- Static Jitter Buffer
- Summary
- Assessment (Quiz): Understanding Jitter

Understanding Jitter

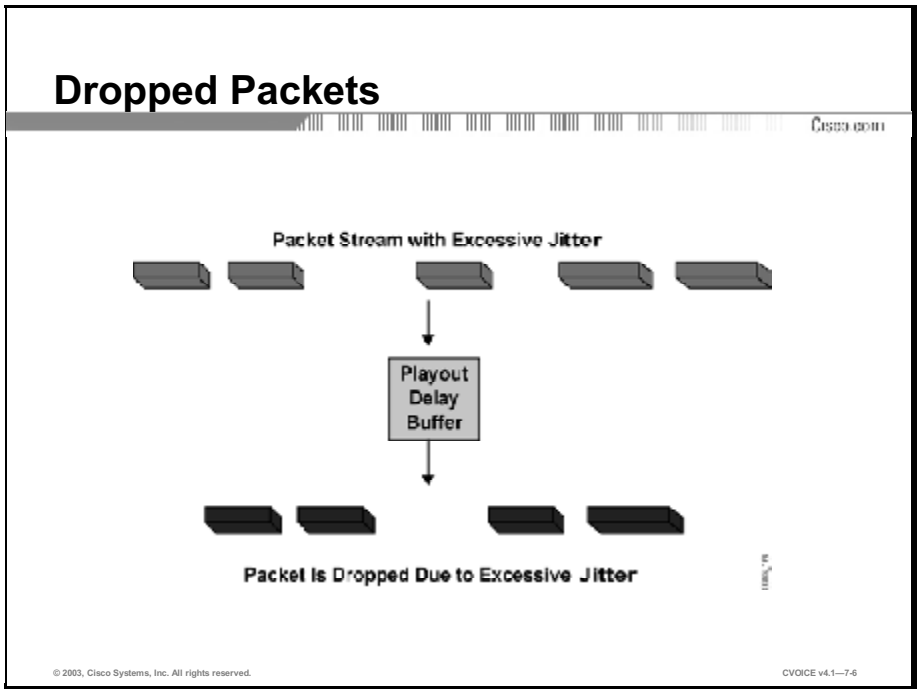
Jitter is an undesirable effect caused by the inherent tendencies of TCP/IP networks and components. This topic describes the cause and effect of jitter.



Jitter is defined as a variation in the delay of received packets. The sending side transmits packets in a continuous stream and spaces them evenly apart. Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant, as shown in the figure. This variation causes problems for audio playback at the receiving end. Playback may experience gaps while waiting for the arrival of variable delayed packets.



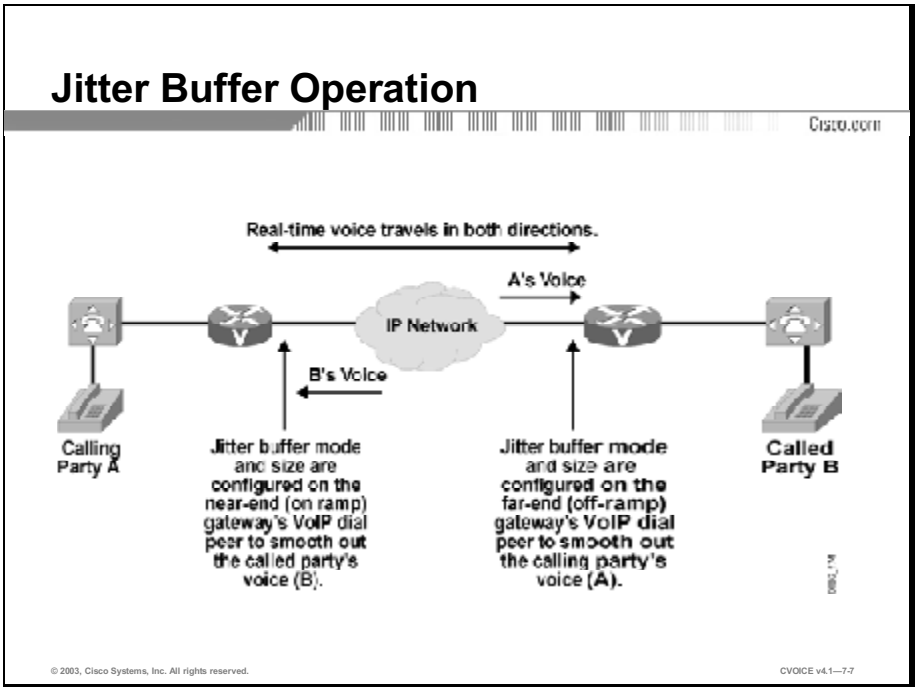
When a router receives an audio stream for Voice over IP (VoIP), it must compensate for any jitter that it detects. The playout delay buffer mechanism handles this function. Playout delay is the amount of time that elapses between the time a voice packet is received at the jitter buffer on the digital signal processor (DSP) and the time a voice packet is played out to the coder-decoder (codec). The playout delay buffer must buffer these packets and then play them out in a steady stream to the DSPs. The DSPs then convert the packets back into an analog audio stream. The playout delay buffer is also referred to as the dejitter buffer.



If the magnitude of jitter is so great that packets are received out of range of the buffer, the out-of-range packets are discarded and dropouts appear in the audio. For losses as small as one packet, the DSP interpolates what it calculates the audio should be, making the problem inaudible through the Cisco IOS® Packet Loss Concealment (PLC) service.

Overcoming Jitter

Cisco voice networks compensate for jitter by setting up a buffer, called the “jitter buffer,” on the gateway router at the receiving end of the voice transmission. This topic explains how to overcome jitter.



The jitter buffer receives voice packets from the IP network at irregular intervals. Occasionally, the voice packets are out of sequence. The jitter buffer holds the packets briefly, reorders them if necessary, and then plays them out at evenly spaced intervals to the decoder in the DSP on the gateway. Algorithms in the DSP determine the size and behavior of the jitter buffer based on user configuration and current network jitter conditions. The DSP uses this information to maximize the number of correctly delivered packets and minimize the amount of delay.

The size of the jitter buffer and the amount of delay is configurable by the user with the **playout-delay** command. Proper configuration is critical. If voice packets are held for too short a time, variations in delay may cause the buffer to underrun (become empty) and cause gaps in speech. However, packets that arrive at a full buffer are dropped, also causing gaps in speech.

To improve voice quality, the speech gaps are hidden by several different techniques that synthesize packets to replace those that were lost or not received in time. Depending on the contiguous duration of the gaps, the missing voice frames are replaced by prediction from the past frames (usually the last frame), followed by silence if the condition persists (more than 30 to 50 ms, for example). The **show call active voice** command output gives buffer overflow and concealment statistics, which are a good indication of the network effect on audio quality.

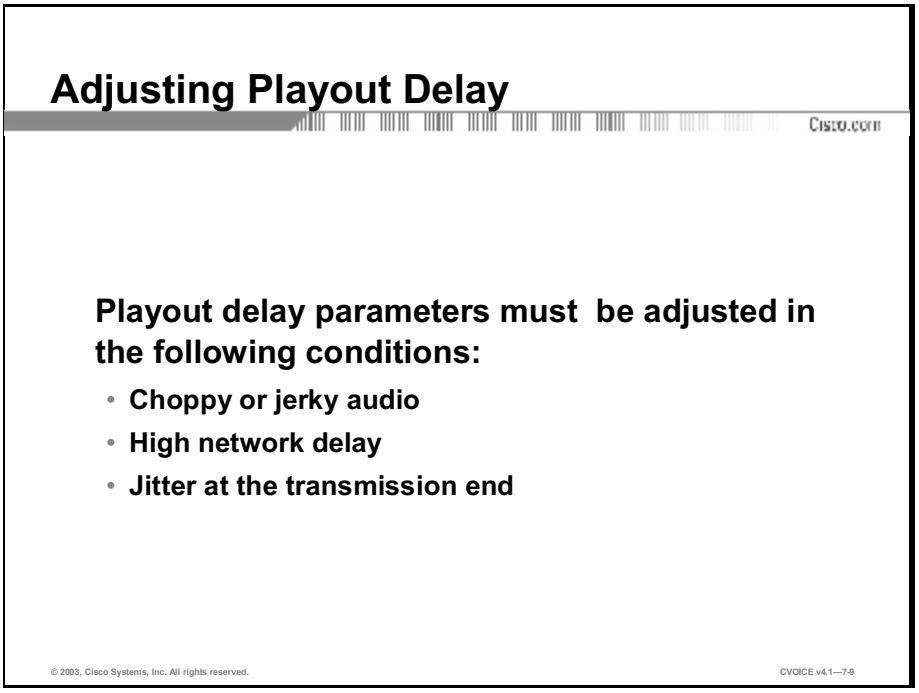
Example

In an example that demonstrates how packets can be lost, a jitter buffer is configured with a maximum playout delay of 40 ms. On the network, packets are delayed from their source; perhaps a media server stops sending packets for 60 ms, or there is severe network congestion. The jitter buffer empties while waiting for input from the network. Input does not arrive until *after* the maximum playout delay time is reached and there is a noticeable break in voice transmission. Now, the media server sends packets *to* the jitter buffer at a faster rate than the packets *leave* the jitter buffer; this makes the jitter buffer fill up. The jitter buffer discards subsequent packets, resulting in a choppy voice signal.

Even though the size of the jitter buffer is configurable, it is important to note that if the buffer size is too large, the overall delay on the connection may rise to unacceptable levels. You must weigh the benefit of improving jitter conditions against the disadvantage of increasing total end-to-end delay, which can also cause voice quality problems.

Adjusting Playout Delay Parameters

This topic lists the symptoms that lead to adjusting playout delay parameters.



The conditions that require you to adjust playout delay parameters are as follows:

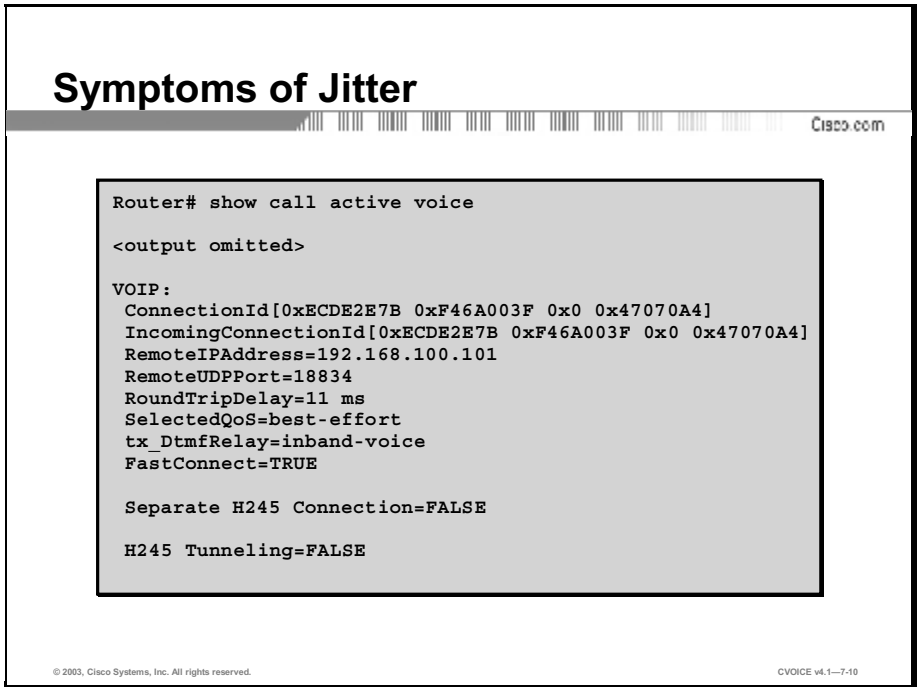
- Gaps in speech patterns that produce choppy or jerky audio suggest that you should increase the minimum playout delay, increase the maximum playout delay, or both, if you are using adaptive mode. For fixed mode, you must increase the nominal value.

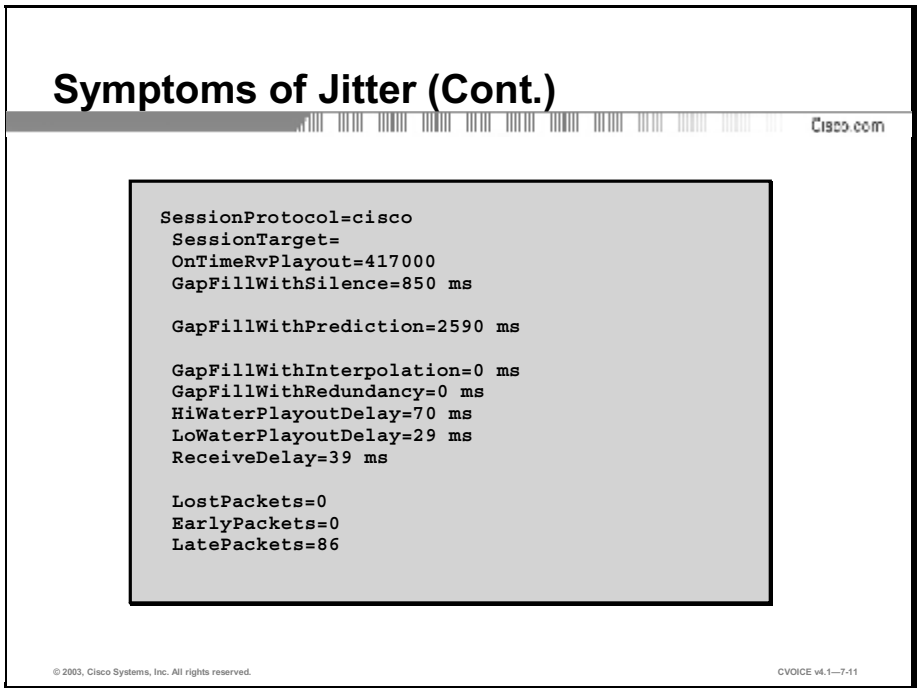
- High overall network delay suggests that you should reduce the maximum playout delay in adaptive mode, or reduce the nominal delay in fixed mode. You must watch for loss of voice quality. The maximum delay value sets an upper limit on adaptive playout delay, which in many cases is the major contributor to end-to-end delay. In many applications, it may be preferable to have the system or the user terminate the call, rather than allow an arbitrarily large delay. The data received with jitter outside this limit will show up in the late packet count in the **show call active voice** playout statistics.

- A noisy but well-understood network or interworking with an application that has lots of jitter at the transmission end, such as a unified messaging server or interactive voice response (IVR) application, suggests selection of fixed mode.

Symptoms of Jitter on a Network

This topic provides examples of output for the **show call active voice** command, which can be used to determine the size of jitter problems.





The figure shows sample output for the **show call active voice** command. Several fields in the **show call active voice** command output that can help you to determine the actual size of the jitter problems are presented in this list:

- **ReceiveDelay:** The playout delay for jitter compensation plus the average expected delay after the frame is available for playout to the decoder. The current low-water mark and high-water mark statistics for the receive delay are available in the output.

- **GapFillWith:** These fields refer to the amount of *concealment*—or packet synthesizing—that took place in this call, to replace the voice packets that were lost or not received in time.

- **LostPackets:** The actual number of packets that were lost; that is, the packets *not* received at the egress gateway. This is detected using the **sequence number** field in the RTP packets.

- **EarlyPackets:** The actual number of packets that arrived *earlier* than the current minimum delay packet. They cause the dejitter algorithm to readjust the minimum delay packet used in jitter estimation.

- **LatePackets:** The actual number of packets that arrived later than the current playout delay setting. The information in these packets is discarded.

Average Jitter Statistics

```
# show call active voice

<output omitted>
.
.
.
VOIP:
 ConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
 IncomingConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
 RemoteIPAddress=192.168.100.101
 RemoteUDPPort=18834
 RoundTripDelay=26 ms
 SelectedQoS=best-effort
 tx_DtmfRelay=inband-voice
 FastConnect=TRUE

 Separate H245 Connection=FALSE

 H245 Tunneling=FALSE
```

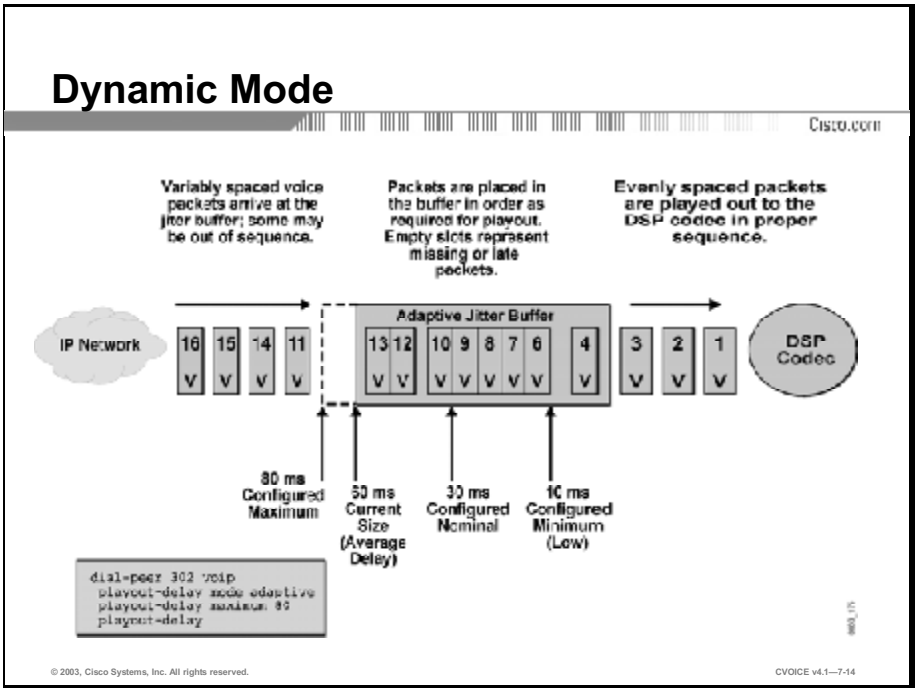

Average Jitter Statistics (Cont.)

```
 SessionProtocol=cisco
 SessionTarget=
 OnTimeRvPlayout=482350
 GapFillWithSilence=1040 ms     <------------  Increased
 GapFillWithPrediction=3160 ms  <------------  Increased
 GapFillWithInterpolation=0 ms
 GapFillWithRedundancy=0 ms
 HiWaterPlayoutDelay=70 ms
 LoWaterPlayoutDelay=29 ms
 ReceiveDelay=43 ms             <------------  Increased
 LostPackets=0
 EarlyPackets=0
 LatePackets=105                <------------  Increased
```


The sample output in this figure displays average jitter statistics when poor voice quality was perceived on the network.

Dynamic Jitter Buffer

This topic describes the dynamic jitter buffer mode.

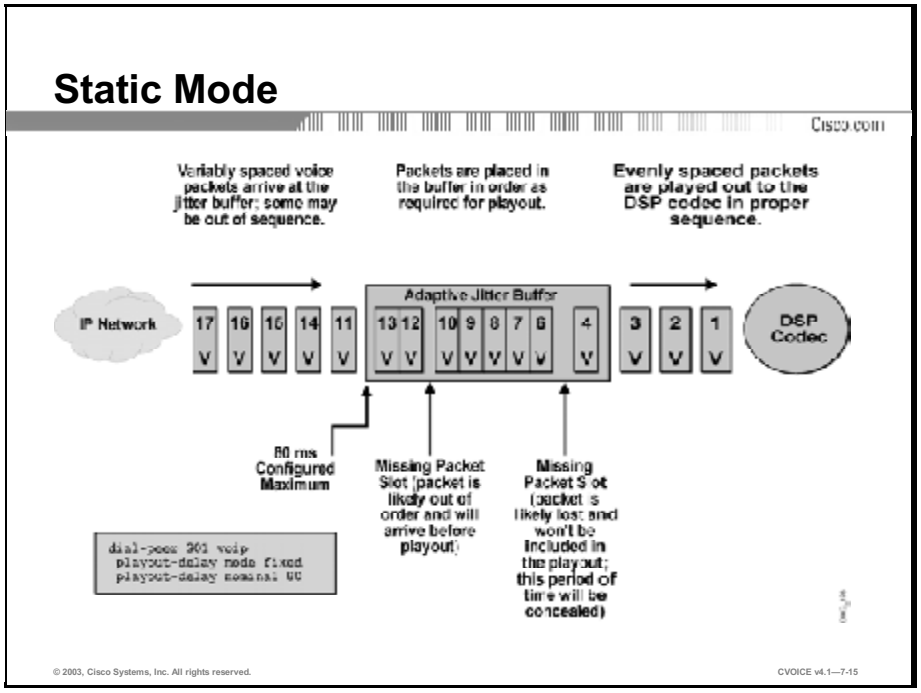


The **playout-delay** command allows you to select a jitter buffer mode (**static** or **dynamic**) and specify certain values that are used by the DSP algorithms to adjust the size of the jitter buffer. During a voice call, the algorithms read time stamps in the Real-Time Transport Protocol (RTP) headers of sample packets to determine the amount of delay that the jitter buffer will apply to an average packet; that is, as if there is no jitter at all in the network. This is called the average delay.

When you configure the **playout-delay mode adaptive** option, the DSP algorithms in the coder-decoder (codec) take samples throughout the voice call and adjust the value of the average delay as network jitter conditions change. The size of the jitter buffer and the amount of delay applied are adjusted upward or downward, as needed. This adjustment ensures the smooth transmission of voice frames to the codec, within the minimum and maximum limits that you configure. The algorithms are designed to reduce the amount of delay *slowly* and increase the amount of delay *quickly* during adjustment. As a result, voice quality is achieved at the risk of larger delay times.

Static Jitter Buffer

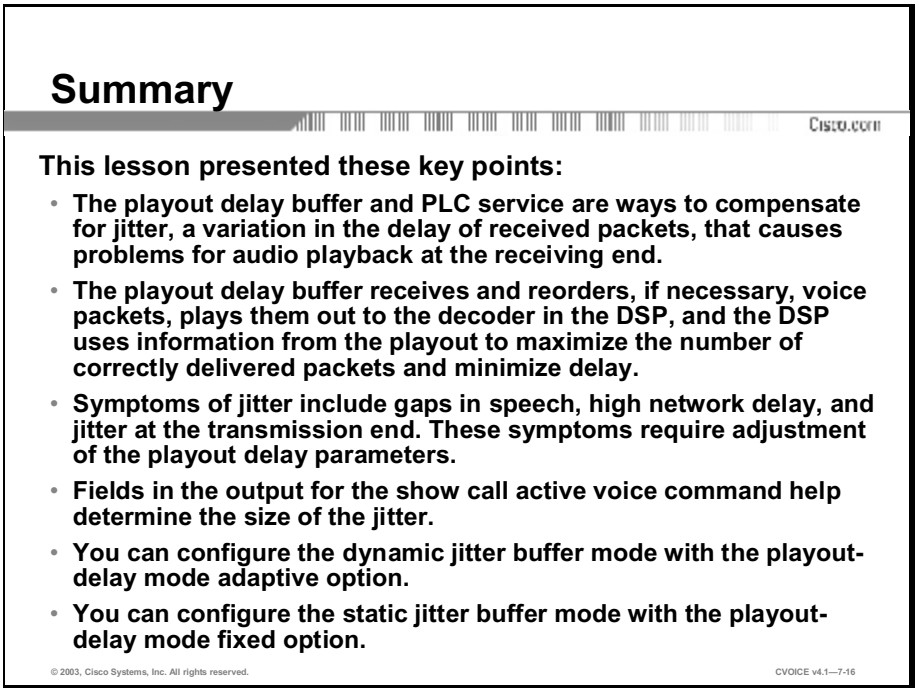
This topic describes the static mode buffer.



When you configure the **playout-delay mode fixed** option, you can specify the nominal delay value, which is the amount of playout delay applied at the beginning of a call by the jitter buffer. This is also the maximum size of the jitter buffer throughout the call.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Understanding Jitter
- Understanding Delay lesson

References

For additional information, refer to these resources:

- "Playout Delay Enhancements for Voice Over IP" http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt_pod.htm
- "Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)" http://www.cisco.com/warp/public/788/voice-qos/jitter_packet_voice.html

Quiz: Understanding Jitter

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz test your knowledge on how to:

- Explain the reasons for jitter in a converged network and list two ways that networks can compensate for it
- Describe the methods used on Cisco Systems voice routers to overcome the problem of jitter
- Identify three symptoms that require the adjustment of playout delay buffer parameters
- Describe all the fields in the **show call active voice** command output that indicate the size of jitter
- Use the **playout-delay mode adaptive** command to configure a dynamic jitter buffer mode
- Use the **playout-delay mode fixed** command to configure a static jitter buffer mode

Instructions

Answer these questions:

Q1) Which device buffers voice packets that arrive with variable delay and plays them out in a steady stream?

A) codec

B) DSP

C) modem

D) playout delay buffer

Q2) Which Cisco IOS service is used to synthesize packets to replace lost packets?

A) DSP

B) IVR

C) PLC

D) switch

Q3) Which device maximizes the number of correctly delivered packets and minimizes delay?

A) codec

B) DSP

C) FXS interface

D) switch

Q4) What may cause gaps in speech on a link that is using a jitter buffer?

A) an empty buffer

B) a full buffer

C) an improperly configured buffer

D) all of the above

Q5) How should you adjust the **playout-delay** parameters for fixed mode if there are gaps in speech?

A) increase the nominal delay

B) increase the minimum playout delay

C) increase the maximum playout delay

D) increase both the minimum and maximum playout delay

Q6) What change should you make to the **playout-delay** configuration if you have excessive jitter at the transmission end?

A) reduce the maximum playout delay

B) increase the minimum playout delay

C) select fixed mode

D) select adaptive mode

Q7) What happens to packets that arrive at the router later than the playout delay setting?

A) They are buffered and sent out in a steady stream.

B) The information in the packets is discarded.

C) They are placed at the head of the egress queue to reduce delay.

D) The packets are revitalized.

Q8) Which command can be used to determine the size of jitter problems?

A) **show jitter**

B) **show call jitter**

C) **show call active voice**

D) **show active voice call**

Q9) Which command is used to enable the codecs to dynamically adjust the value of the average delay depending on network conditions?

A) **playout-delay mode adaptive**

B) **playout-delay mode adjust**

C) **playout-delay mode auto**

D) **playout-delay mode dynamic**

Q10) What information do the DSP algorithms use to determine the amount of delay the jitter buffer applies to a packet?

A) average expected delay after the frame is available for playout

B) statistics from the **show** command used to determine jitter problems

C) sequence number field in the RTP packet

D) time stamps in the RTP headers of a sample of packets

Q11) In fixed mode, what does the nominal delay value signify?

A) the minimum amount of delay that is configurable for each voice packet

B) the amount of delay that is applied by the jitter buffer to each packet

C) the amount of playout delay that is applied by the jitter buffer at the beginning of a call

D) the minimum amount of delay that is applied by the jitter buffer for the duration of the call

Q12) In which mode can you specify the nominal delay value?

A) auto mode

B) adaptive mode

C) fixed mode

D) adaptive and fixed mode

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Understanding Delay

Overview

When designing networks that transport voice over packet, frame, or cell infrastructures, it is important to understand and account for the delay components in the network to ensure acceptable network performance. Overall voice quality is a function of many factors, including the compression algorithm, errors and frame loss, echo cancellation, and delay. This lesson explains the sources of delay when using Cisco routers and gateways over packet networks and proposes solutions for this problem.

Importance

Delay is the worst enemy of Voice over IP (VoIP) networks. Network administrators must have a solid understanding of the causes of delay and the solutions for this problem to successfully implement a VoIP network.

Objectives

Upon completing this lesson, you will be able to:

- Describe the purpose of a delay budget and how delay is measured across a VoIP network
- Use ITU Recommendation G.114 to identify acceptable and unacceptable delay
- Describe the six major factors that contribute to voice packet delay
- Identify best-case and worst-case delays that are associated with different types of coders
- Calculate serialization delay based on packet size and line speed
- Use the **frame-relay fragment** *fragment_size* command to configure fragment size
- Use the delay budget to calculate one-way delay

Learner Skills and Knowledge

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

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

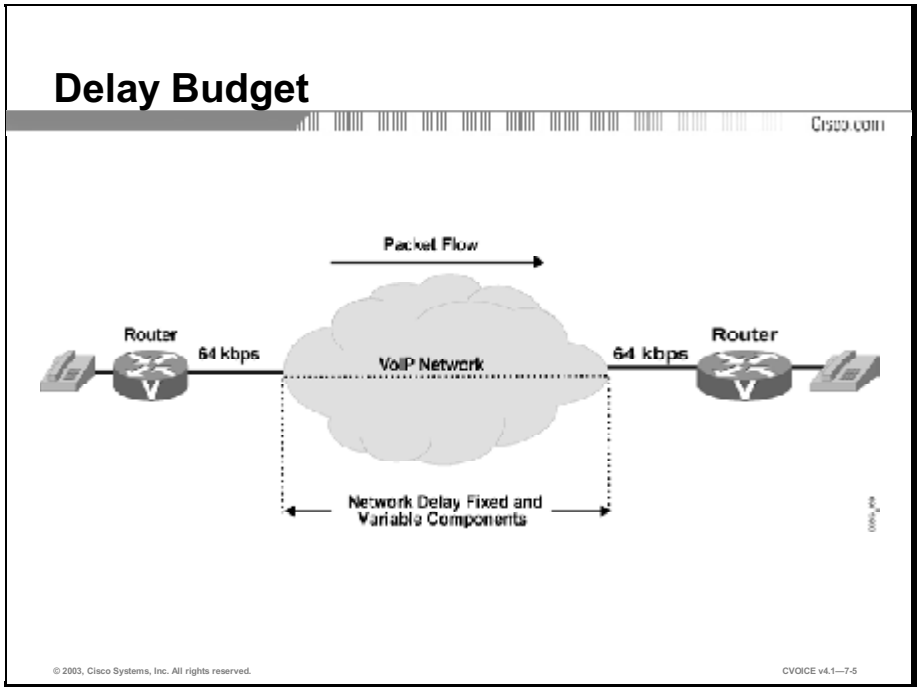
Outline

This lesson includes these topics:

- Overview
- Need for a Delay Budget
- Guidelines for Acceptable Delay
- Sources of Delay
- Effects of Coders and Voice Sampling on Delay
- Managing Serialization Delay
- Managing Queuing Delay
- Verifying End-to-End Delay
- Summary
- Assessment (Quiz): Understanding Delay

Need for a Delay Budget

The end-to-end delay in a VoIP network is known as the delay budget. Network administrators must design a network to operate within an acceptable delay budget. This topic explains the concept of delay budget and how to measure it.



Delay is the accumulated latency of end-to-end voice traffic in a VoIP network. The purpose of a delay budget is to ensure that the voice network does not exceed accepted limits for voice telephony conversation. The delay budget is the sum of all the delays, fixed and variable, that are found in the network along the audio path. You can measure delay budget by adding up all of the individual contributing components, as shown in the figure. The delay budget is measured in each direction individually, not round-trip.

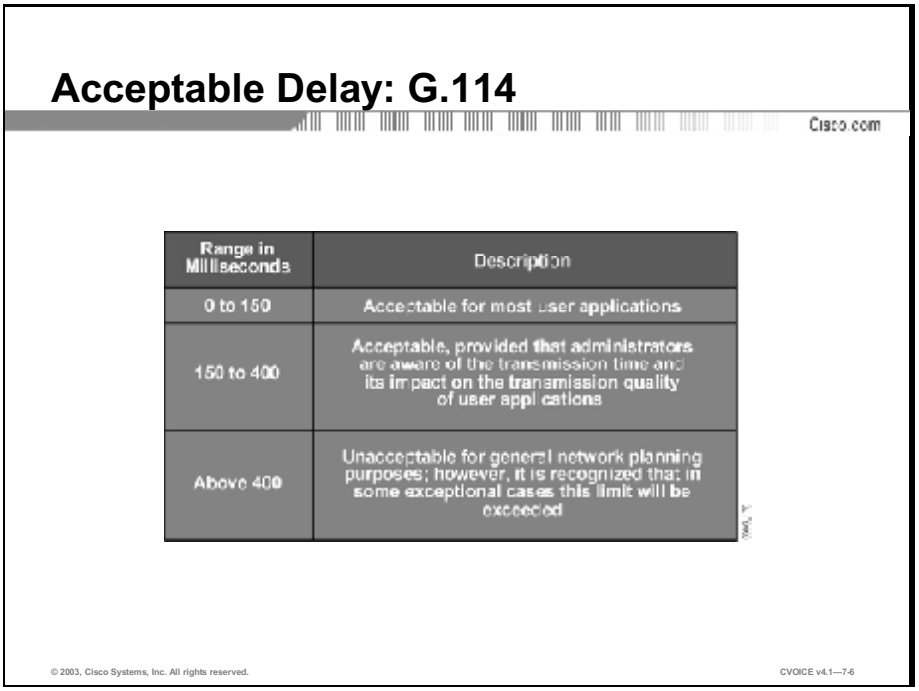
Network administrators must be aware that delay exists, and then design their network to bring end-to-end delay within acceptable limits.

Example

As delay increases, talkers and listeners become unsynchronized and often find themselves speaking at the same time or both waiting for the other to speak. This condition is commonly called *talker overlap*. While the overall voice quality is acceptable, users may find the stilted nature of the conversation unacceptably annoying. Talker overlap may be observed on international telephone calls that travel over satellite connections. Satellite delay is about 500 ms: 250 ms up and 250 ms down.

Guidelines for Acceptable Delay

International telephony communications must adhere to a delay standard. This topic defines the standard and its limits.



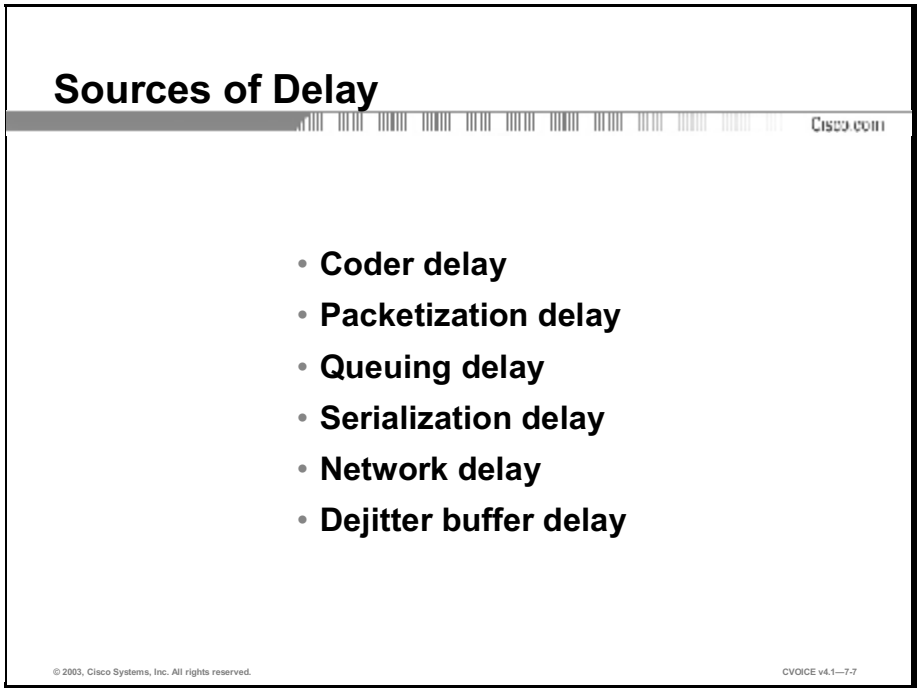
The International Telecommunication Union (ITU) addresses network delay for voice applications in Recommendation G.114. This recommendation is oriented to national telecom administrations and is more stringent than what is normally applied in private voice networks. When the location and business needs of end users are well-known to the network designer, more delay may prove acceptable.

Example

As shown in the figure, acceptable delay time is between 0 to 400 ms for private networks. Delay times that exceed 400 ms are unacceptable for general network planning; however, all networks should be engineered to recognize and minimize the voice-connection delay.

Sources of Delay

Many factors add to overall delay. This topic lists six of these factors.



Following is an explanation of six major factors that contribute to overall fixed and variable delay:

- **Coder delay:** Also called processing delay, coder delay is the time taken by the digital signal processor (DSP) to compress a block of pulse code modulation (PCM) samples. Because different coders work in different ways, this delay varies with the voice coder that is used and the processor speed.

- **Packetization delay:** Packetization delay is the time it takes to fill a packet payload with encoded or compressed speech. This delay is a function of the sample block size that is required by the vocoder and the number of blocks placed in a single frame. Packetization delay is also called accumulation delay because the voice samples accumulate in a buffer before being released. With typical payload sizes used on Cisco Systems routers, packetization delay for G.711, G.726, and G.729 does not exceed 30 ms.

- **Queuing delay:** After the network builds a compressed voice payload, it adds a header and queues for transmission on the network connection. Because voice should have absolute priority in the router or gateway, a voice frame must wait only for a data frame already playing out or for other voice frames ahead of it. Essentially, the voice frame waits for the serialization delay of any preceding frames that are in the output queue. Queuing delay is a variable delay and is dependent on the trunk speed and the state of the queue.

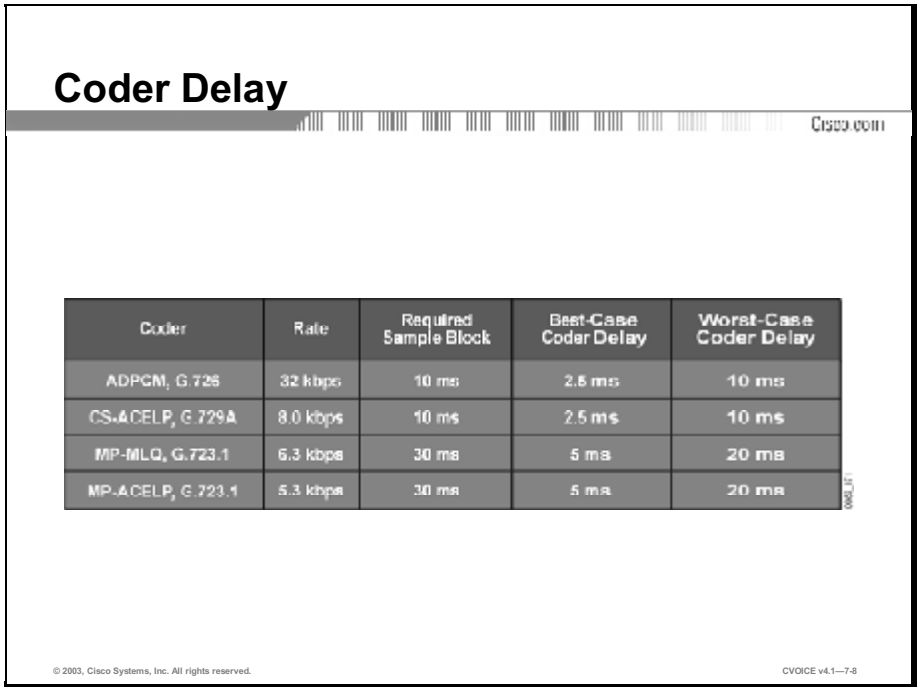
- **Serialization delay:** Serialization delay is the fixed delay that is required to clock a voice or data frame onto the network interface; it is directly related to the clock rate on the trunk.

- **Network delay:** The public Frame Relay or ATM network that interconnects the endpoint locations is the source of the longest voice-connection delays. These delays are also the most difficult to quantify. If Cisco (or some other private network) provides wide-area connectivity, it is possible to identify the individual components of delay. In general, the fixed components are from propagation delays on the trunks within the network; variable delays are the result of queuing delays that clock frames into and out of intermediate switches. To estimate propagation delay, a popular estimate of 10 microseconds/mile or 6 microseconds/km (G.114) is widely used, although intermediate multiplexing equipment, backhauling, microwave links, and other features of carrier networks create many exceptions. Typical carrier delays for U.S. Frame Relay connections are 40 ms fixed, and 25 ms variable, for a total worst-case delay of 65 ms.

- **Dejitter buffer delay:** Because speech is a constant bit-rate service, the jitter from all the variable delays must be removed before the signal leaves the network. In Cisco routers and gateways, this is accomplished with a dejitter buffer at the far-end (receiving) router or gateway. The dejitter buffer transforms the variable delay into a fixed delay by holding the first sample that is received for a period of time *before* playing it out. This holding period is known as the initial playout delay. The actual contribution of the dejitter buffer to delay is the initial playout delay of the dejitter buffer *plus* the actual amount of delay of the first packet that was buffered in the network. The worst case would be twice the dejitter buffer initial delay (assuming the first packet through the network experienced only minimal buffering delay).

Effects of Coders and Voice Sampling on Delay

The process of encoding an analog voice sample into a compressed digitized bit stream contributes to delay. This topic describes the effect of coder delay. Best and worst-case coder delays are shown in the figure.

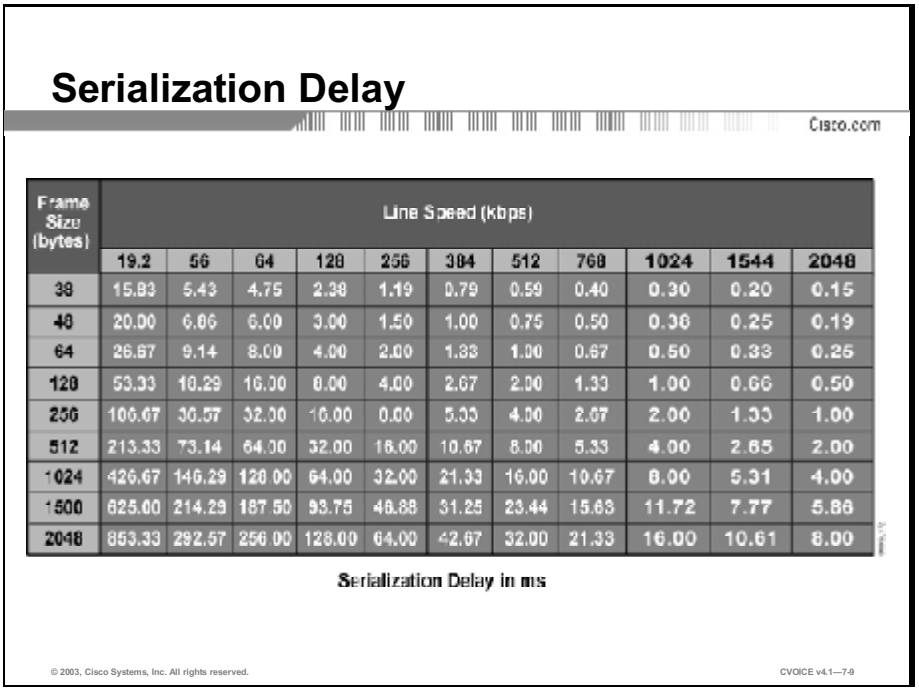


The compression time for a conjugate structure algebraic code excited linear prediction (CS-ACELP) process ranges from 2.5 to 10 ms, depending on the loading of the DSP. If the DSP is fully loaded with four voice channels, the coder delay will be 10 ms. If the DSP is loaded with one voice channel only, the coder delay will be 2.5 ms. For design purposes, we will use the worst-case time of 10 ms.

Decompression time is roughly 10 percent of the compression time for each block. However, because there may be multiple samples in each frame, the decompression time is proportional to the number of samples per frame. Consequently, the worst-case decompression time for a frame with three samples is 3 * 1 ms or 3 ms. Generally, two or three blocks of compressed G.729 output are put in one frame, while only one sample of compressed G.723.1 output is sent in each frame.

Managing Serialization Delay

An important part of delay is the serialization delay on the interface. This topic describes serialization delay and its management.



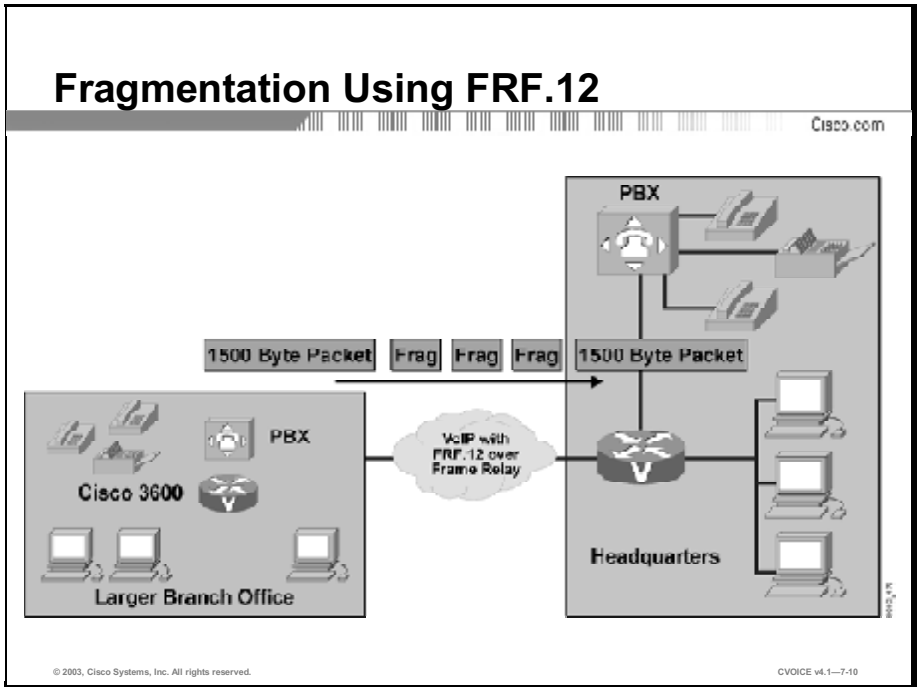
The figure shows the serialization delay required for different frame sizes at various line speeds. This table uses total frame size, not payload size, for computation. As an example, reading from the graphic, on a 64-kbps line, a CS-ACELP voice frame with a length of 38 bytes (37 bytes + 1-byte flag) has a serialization delay of 4.75 ms. If the line speed is increased to 1.544 Mbps, the serialization delay goes down to 0.2 ms. Cisco recommends a 10-ms serialization delay, not to exceed 20 ms.

You can effectively change the serialization delay of a voice packet by performing the following:

- Increasing the link speed
- Decreasing the packet size

Managing Queuing Delay

Queuing delay contributes to overall delay. This topic explains queuing delay and offers a standard solution.



Queuing delay occurs when other elements in the outbound queue (voice or data packets) cause voice packets to be delayed; for example, the serialization delay for a 1500-byte packet is 214 ms to leave the router over a 56-kbps link. If a 1500-byte data packet that is not real-time is being sent, real-time (voice) packets are queued until the large data packet is transmitted. This delay is unacceptable for voice traffic. If not real-time data packets are fragmented into smaller frames, they are interleaved with real-time (voice) frames. In this way, both voice and data frames can be carried together on low-speed links without causing excessive delay to the real-time voice traffic. One way to implement this fragmentation is to use FRF.12 on VoIP over Frame Relay networks. FRF.12 serves to fragment Frame Relay frames into smaller frames, even from different permanent virtual circuits (PVCs).

Fragment Size Configuration

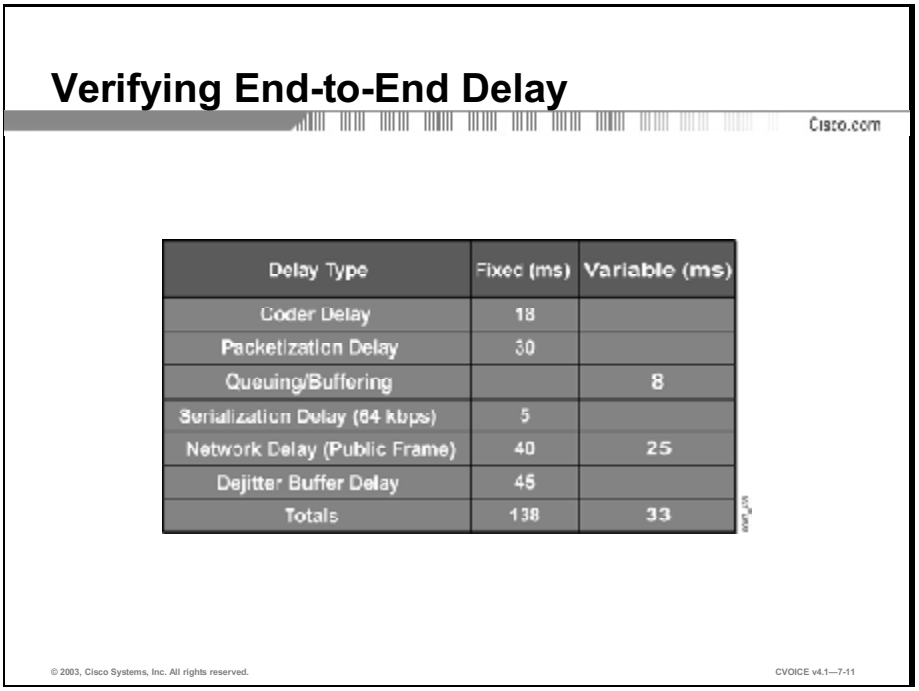
You can configure fragment size using the **frame-relay fragment** *fragment_size* command in a Frame Relay map class. The “fragment_size” defines the payload size of a fragment, and excludes the Frame Relay headers and any Frame Relay fragmentation header. The valid range is from 16 to 1600 bytes; the default is 53 bytes.

The **“**fragment_size” should be set so that the serialization delay is not more than 10 ms. For example, if using a using a 384-kbps link, the fragmentation size should be set at 512 kbps.

Set the fragmentation size so that the largest data packet is not larger than the voice packets.

Verifying End-to-End Delay

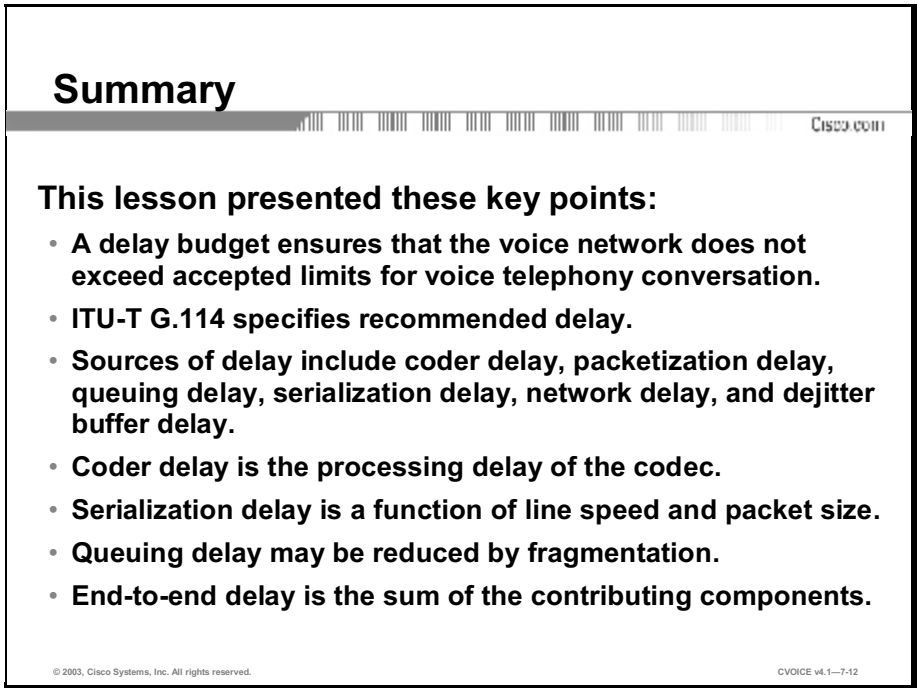
End-to-end delay is calculated and compared to the G.711 recommendation. This topic illustrates the process.



A typical one-hop connection over a public Frame Relay connection may have the delay budget that is shown in the figure. To calculate one-way delay, simply add all of the contributing components together. The goal is to allow a one-way delay as recommended by G.114. The figure shows an acceptable one-way delay of 138 ms, plus 33 ms, for a total of 171 ms.

Summary

This topic summarized the key points discussed in this lesson



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Understanding Delay
- Applying Quality of Service in the Campus lesson

References

For additional information, refer to these resources:

- "Understanding Delay in Packet Voice Networks" http://www.cisco.com/warp/public/788/voip/delay-details.html#60

Quiz: Understanding Delay

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the purpose of a delay budget and how delay is measured across a VoIP network
- Use ITU Recommendation G.114 to identify acceptable and unacceptable delay
- Describe the six major factors that contribute to voice packet delay
- Identify best-case and worst-case delays that are associated with different types of coders
- Calculate serialization delay based on packet size and line speed
- Use the **frame-relay fragment** *fragment_size* command to configure fragment size
- Use the delay budget to calculate one-way delay

Instructions

Answer these questions.

Q1) What is the purpose of a delay budget?

A) to synchronize voice traffic

B) to provide guaranteed delay for voice packets

C) to ensure that voice traffic does not exceed accepted limits for delay

D) to provide quality of service services

Q2) What is the delay budget for a network?

A) the sum of fixed and variable delay from end to end for each direction

B) the sum of the one-way fixed and variable delay

C) the sum of the round-trip fixed and variable delay calculated between each device

D) the sum of the fixed and variable delay between the egress and ingress router in both directions

Q3) According to ITU-T Recommendation G.114, what is the acceptable delay for national telecom administrations?

A) 0 to 150 ms

B) 0 to 400 ms

C) 150 to 400 ms

D) above 400 ms

Q4) According to ITU-T Recommendation G.114, what is the acceptable delay for private networks?

A) 0 to 150 ms

B) 0 to 400 ms

C) 150 to 400 ms

D) above 400 ms

Q5) Match the factor that contributes to delay with its description.

A) coder delay

B) packetization delay

C) serialization delay

D) dejitter buffer delay

_____ 1. time taken to fill a packet payload with encoded speech

_____ 2. time required to clock a frame onto the network interface

_____ 3. time taken by the DSP to compress a block of PCM samples

_____ 4. time a sample is held before being played out

Q6) Which factor contributes most to variable delay on the network?

A) dejitter buffer delay

B) serialization delay

C) packetization delay

D) queuing delay

Q7) What will be the coder delay if a G.726 is loaded with four channels?

A) 2.5 ms

B) 5 ms

C) 10 ms

D) 20 ms

Q8) What is the decompression time for each sample block of voice traffic?

A) roughly twice the compression time for each block

B) roughly 3 times the compression time for each block

C) roughly 3 percent of the compression time for each block

D) roughly 10 percent of the compression time for each block

Q9) How much serialization delay is recommended by Cisco?

A) 0.2 ms

B) 0.5 ms

C) 10 ms

D) 20 ms

Q10) Identify two ways to reduce serialization delay? (Choose two.)

A) by increasing packet compression

B) by reducing the processing delay

C) by increasing the link speed

D) by prioritizing the packets

E) by decreasing the packet size

F) by reducing the queuing delay

Q11) What factors should you consider when setting the fragment size in the **frame-relay fragment** command?

A) The payload size is between 16 and 1600 bytes.

B) The serialization delay is not more than 10 ms.

C) The largest data packet is not larger than the voice packets.

D) All of the above.

Q12) Which type of delay directly affects queuing delay?

A) coder delay

B) network delay

C) serialization delay

D) packetization delay

E) dejitter buffer delay

Q13) Which two factors contribute to fixed delay only? (Choose two.)

A) coder delay

B) network delay

C) queuing delay

D) packetization delay

Q14) Which ITU-T Recommendation is considered to be a measure of acceptable end-to-end delay?

A) G.114

B) G.115

C) G.711

D) G.411

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Applying Quality of Service in the Campus

Overview

This lesson covers introductory design considerations and recommendations for implementing quality of service (QoS) in a campus environment. For in-depth training on QoS in a campus environment, students are referred to Cisco *Quality of Service* courses.

Importance

Until recently, many network experts believed that QoS would never be an issue in the campus because bandwidth availability, buffer overflow and the bursty nature of network traffic. Gradually, network administrators have realized that buffering, not bandwidth, is the dominant issue in the campus. For this reason, QoS tools are required to manage these buffers to minimize loss, delay, and delay variation.

Objectives

Upon completing this lesson, you will be able to:

- Identify the areas of a campus network that require QoS services
- Describe separation of queues as an approach to QoS management in a campus network
- Describe queue scheduling as an approach to QoS management in a campus network
- Describe marking control and management traffic as an approach to QoS management in a campus network.
- Provide an example of a QoS configuration on a campus network
- Describe three queuing and scheduling methods

- Configure switch-wide queuing and mark control and management traffic in a campus network

Learner Skills and Knowledge

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

- Basic knowledge of Voice over IP (VoIP) concepts
- Knowledge of Cisco IOS® software
- Knowledge of Cisco Catalyst® switches
- Knowledge of campus networks

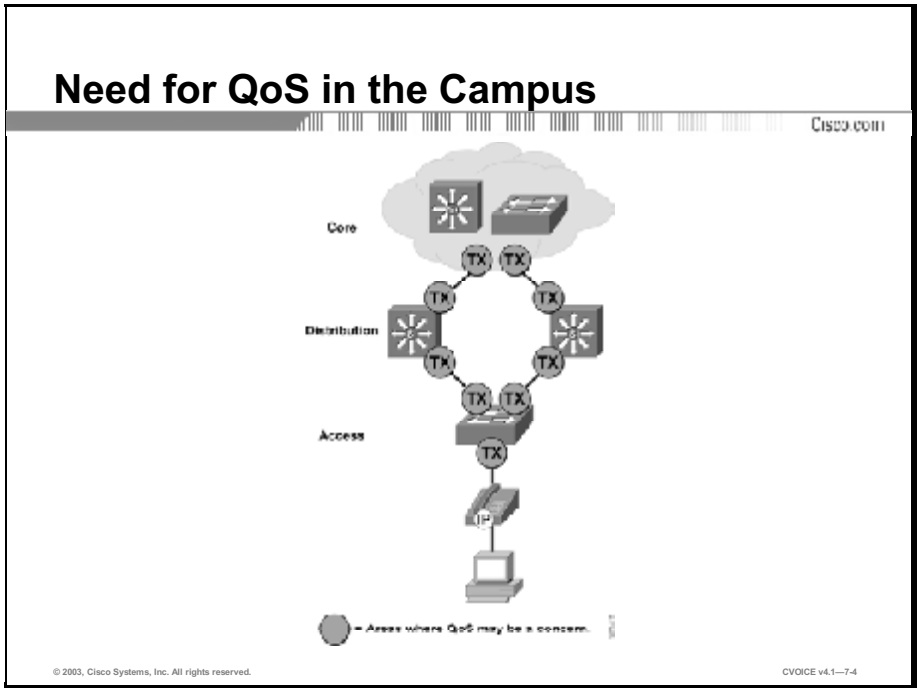
Outline

This lesson includes these topics:

- Overview
- Need for QoS in the Campus
- Separation of Queues
- Queue Scheduling
- Marking Control and Management Traffic
- Configuring QoS in the Campus
- Separation and Scheduling of Queues
- Configuration Examples
- Summary
- Assessment (Quiz): Applying Quality of Service in the Campus

Need for QoS in the Campus

This topic describes the need for Quality of Service (QoS) measures in a campus network.



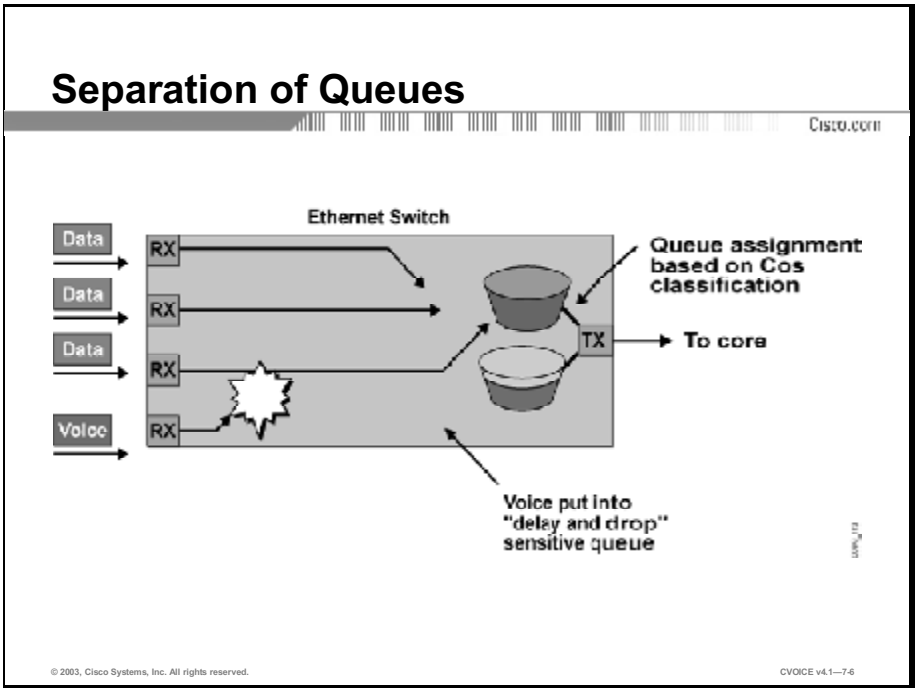
The bursty nature of data networks, combined with the high volume of smaller TCP packets, cause transmit buffers fill to capacity in high-speed campus networks. If an output buffer fills, ingress interfaces are unable to place new flow traffic into the output buffer. When the ingress buffer is filled, which can happen quickly, packet drops occur. Typically, these drops are more than a single packet in any given flow. TCP packet loss causes retransmissions to occur, further aggravating the problem. Voice packet loss results in voice clipping and skips.

The figure illustrates the areas of a campus network where QoS is a concern. These areas are as follows:

- **Access ports:** Access-level ports that connect to IP Phones or gateways and the distribution switches.
- **Distribution ports:** Uplink ports that connect to access switches and core switches.
- **Core ports:** Uplink ports that connect the distribution switches to the core campus switches.

Separation of Queues

This topic explains how you can use multiple queues to avoid dropped packets.

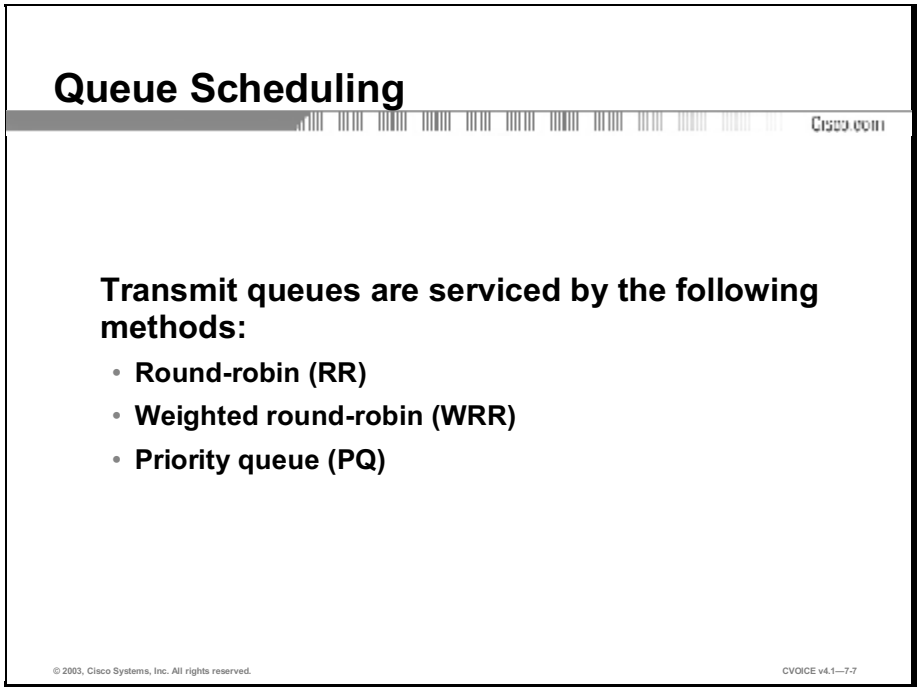


VoIP traffic is sensitive to both delayed packets and dropped packets. Even though a campus may be using gigabit Ethernet trunks, which have extremely fast serialization times, delay and dropped packets may still be an issue because of the speed and capacity of the gigabit Ethernet trunk. However, drops *always* adversely affect voice quality in the campus. Using multiple queues on transmit interfaces is the only way to eliminate the potential for dropped traffic caused by buffers operating at 100 percent capacity. By separating voice (which is sensitive to delays and drops) into its own queue, you can prevent flows from being dropped at the ingress interface even if data flows fill up the data transmit buffer. If video is present, it should also have its own queue because it has similar delay characteristics.

Caution	It is critical that you verify that flow control is disabled when enabling QoS (multiple queues) on Catalyst switches. Flow control interferes with the configured queuing behavior by acting on the ports before activation of queuing. Flow control is disabled by default.

Queue Scheduling

Queues should schedule packet dispatching to ensure the emptying of queues in a fair and timely fashion. This topic describes queue scheduling as an approach to management of QoS in a campus network.

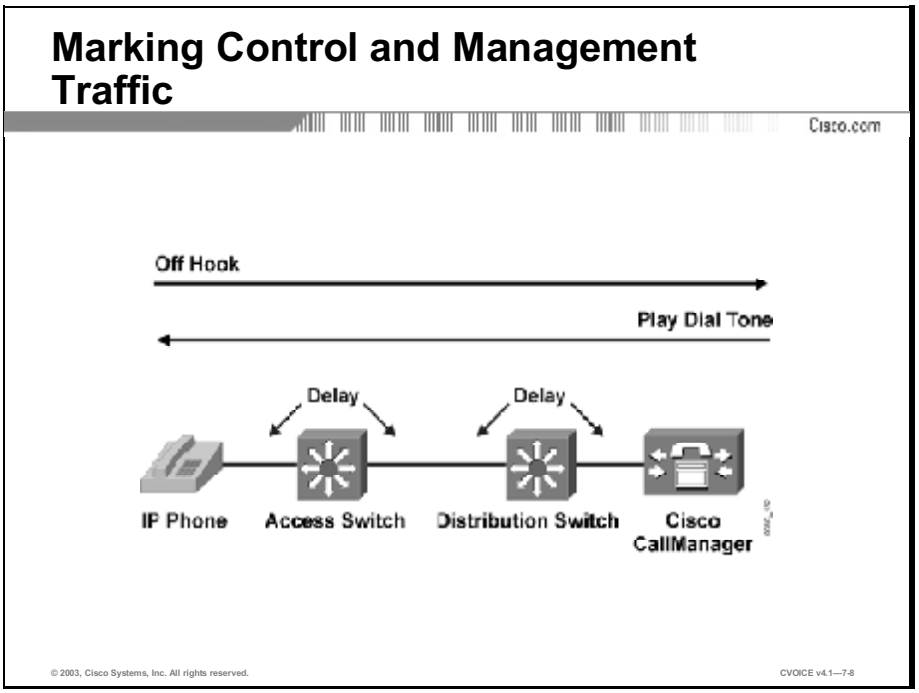


The scheduler process consists of a variety of methods to service each of the transmit queues (voice and data). The easiest method is a round-robin (RR) algorithm, which services queue 1 through queue N in a sequential manner. While not robust, this is an extremely simple and efficient method that you can use for branch office and wiring-closet switches. Distribution layer switches use a weighted round-robin (WRR) algorithm in which higher priority traffic is given a scheduling "weight." WRR provides bandwidth to higher priority applications using IP precedence and grants access to lower priority queues. The frame schedule affords the bandwidth that each queue is allotted by the network administrator. This mapping is configurable, both at the system and interface levels. Care should be taken when configuring WRR as it may affect bandwidth provided to other lower-priority queues.

Another option is to combine RR or WRR scheduling with priority scheduling for applications that are sensitive to packet delay and drop. This uses a priority queue (PQ) that is always served first when there are packets in the queue. If there are no frames in the PQ, the additional queues are scheduled using RR or WRR. You should take care when implementing a PQ as it may "starve" traffic in lower queues if there is too much priority traffic.

Marking Control and Management Traffic

Marking control and management traffic is critical to the VoIP network performance. Control and management traffic should be marked for preferential dispatching throughout the campus. This topic describes marking control and management traffic as an approach to the management of QoS in a campus network.

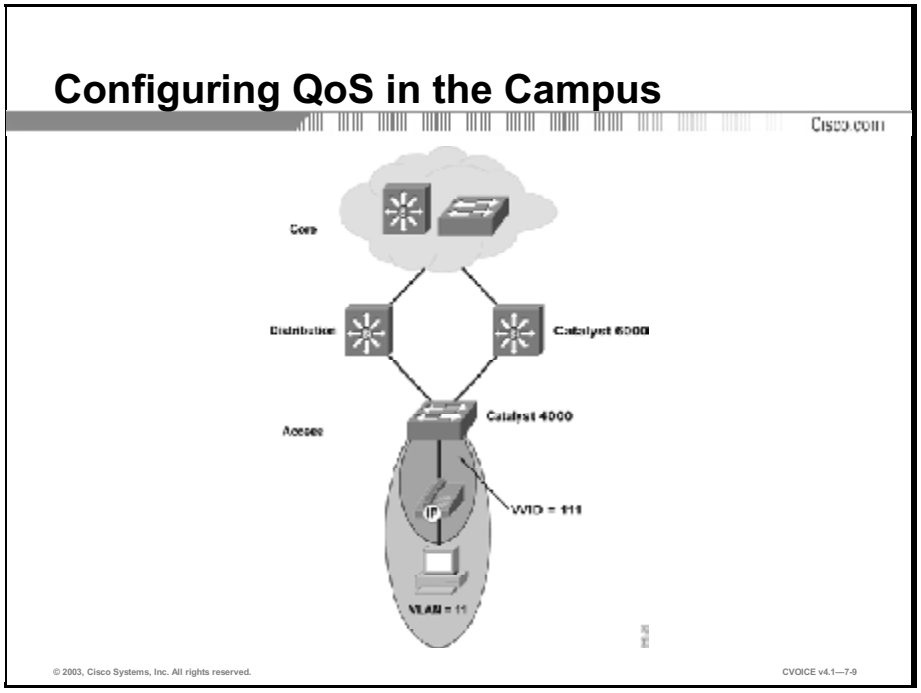


In networks with high-traffic loads, managing the delivery of control traffic is critical to ensuring a positive user experience with VoIP. Delay to Dial-Tone (DTT) time is an example of this type of delivery management. When a Cisco IP Phone goes off hook, it “asks” Cisco CallManager for instructions. Cisco CallManager then instructs the Cisco IP Phone to play a dial tone. If this management and control traffic is dropped or delayed within the network, the user experience is adversely affected. The same logic applies to all signaling traffic for gateways and telephones.

To ensure that this control and management traffic is marked as important (but not as important as the actual RTP stream), access control lists (ACLs) are used to classify these streams on Catalyst 3500, 4000, and 6000 switches that are enabled for Layers 3 and 4.

Configuring QoS in the Campus

This topic describes how to configure QoS in a campus network.



The figure illustrates a network. Note that the access switch is a Catalyst 4000 and the distribution and core switches are Catalyst 6000. Also note that the Cisco IP Phone operates in voice VLAN ID (VVID) 111, while the workstation operates in voice VLAN 11. VLAN increases the quality of the voice traffic and allows a large number of telephones to be added to an existing network (where there are not enough IP addresses), by isolating the telephones on a separate auxiliary. A new VLAN means a new subnet and a new set of IP addresses.

In the access-switch configuration, the distribution and core switches must also be configured; however, the configuration is very similar to the access-switch configuration

Configuring a Voice VLAN

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport voice vlan 101
Router(config-if)# exit
```


The figure shows how to configure Fast Ethernet port 5/1 to send CDP packets that tell the Cisco IP Phone to use VLAN 101 as the voice VLAN.

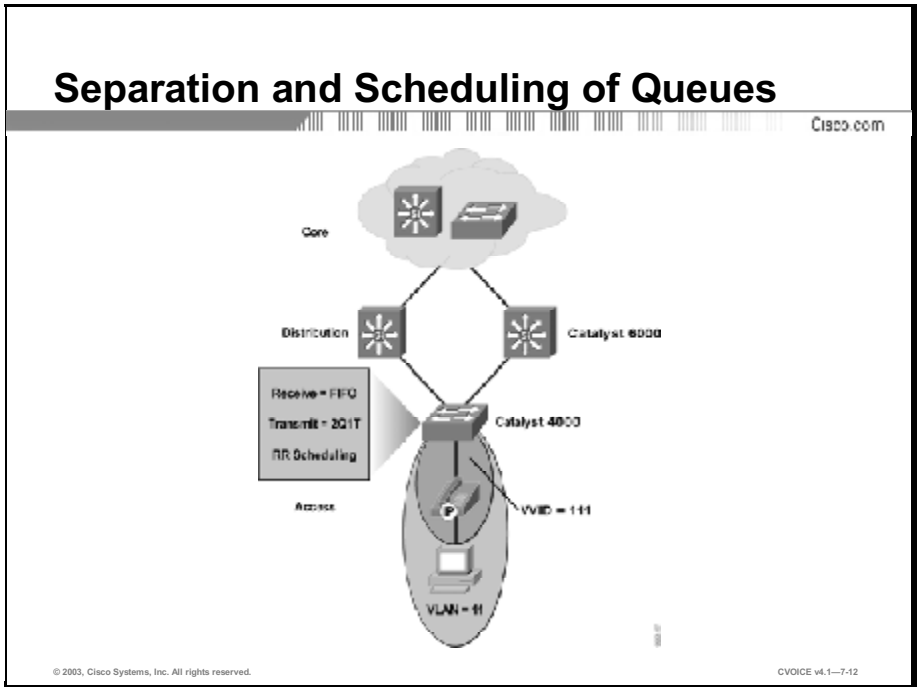
Verifying the Configuration

```
Router# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: access
Operational Mode: access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 100
Voice VLAN: 101
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 900 ((Inactive)) 901
((Inactive))
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```


This example shows how to verify the configuration of Fast Ethernet port 5/1.

Separation and Scheduling of Queues

This topic presents several suggested configurations for port scheduling and queuing on the Catalyst 4000 at the access layer.



Switch-Wide Queuing

Configuration for switch-wide queuing depends upon the type of interface that is used. The two types of interfaces used are:

- **Receive interface:** The recommended configuration for the receive interface is one standard FIFO queue.

- **Transmit interface:** The recommended configuration for the transmit interface is two standard queues with a single threshold (2Q1T). This method is preferred over other methods because it places traffic with specific class of service (CoS) in one queue (as configured) and all other traffic in the second queue, thus simplifying configuration. The threshold indicates that traffic is dropped when the buffer capacity reaches 100 percent. Scheduling is done on an RR basis. Admission to the queues is based on the 802.1p CoS value and is user-configurable in pairs. If you enable QoS, but do not modify the CoS-to-transmit queue mappings, switch performance could be affected because all traffic goes to queue 1.

Note	802.1p is a Layer 2 mechanism for classifying traffic using 3 bits. 802.1p adds 16 bits to the Layer 2 header.

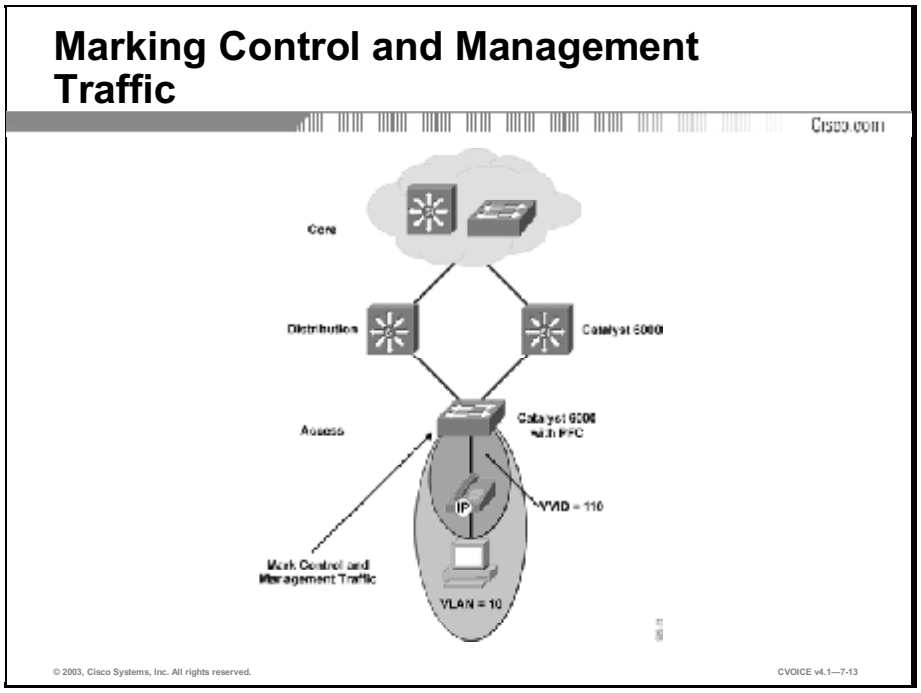
IP Phone Port Queuing

In Catalyst OS (CatOS) Software Release 5.5.1, the Catalyst 4000 line does not offer any advanced IP Phone-queuing features. Because of this, the Catalyst 4000 depends on the default CoS marking and enforcement on the Cisco IP Phone. Other access switches (such as the Catalyst 3500), offer more advanced IP port phone-queuing options.

Uplink Interface to the Distribution Switch

You do not need to configure special queuing or scheduling commands on the Catalyst 4000 side of the link (from the access layer Catalyst 4000 to the distribution layer Catalyst 6000). Queuing is automatically enabled (after QoS has been enabled) and the classification and queue admission have been configured.

Marking Control and Management Traffic

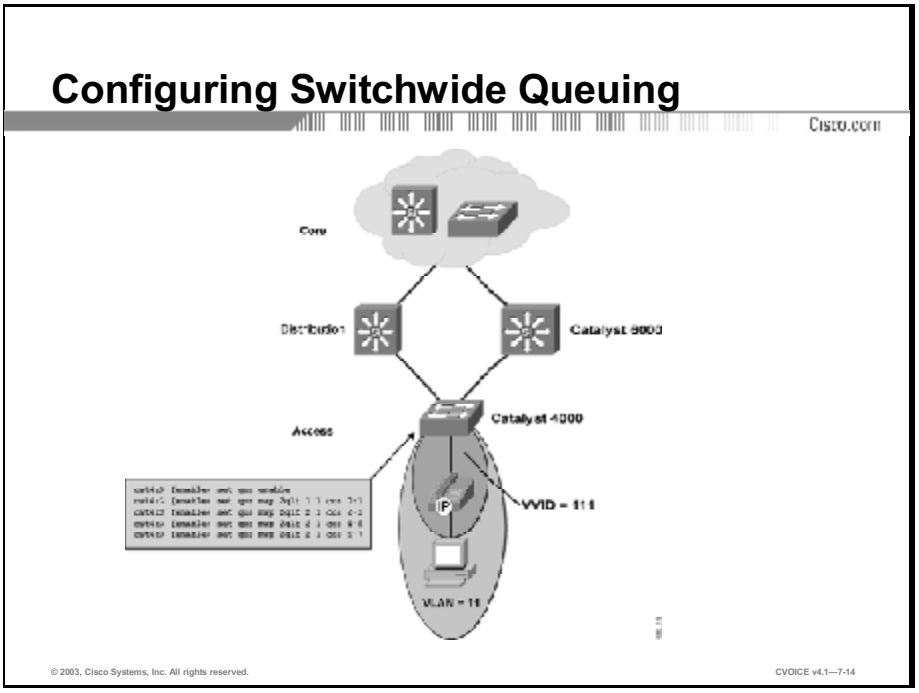


If the access switch is a Catalyst 5000 or 6000, you can classify control and management traffic in the campus. To ensure that this control and management traffic is marked as important (but not as important as the actual RTP stream), ACLs are used to classify these streams on Catalyst 5000 and 6000 switches that are enabled for Layers 3 and 4. You should enable this classification and marking for all capable switches in the campus.

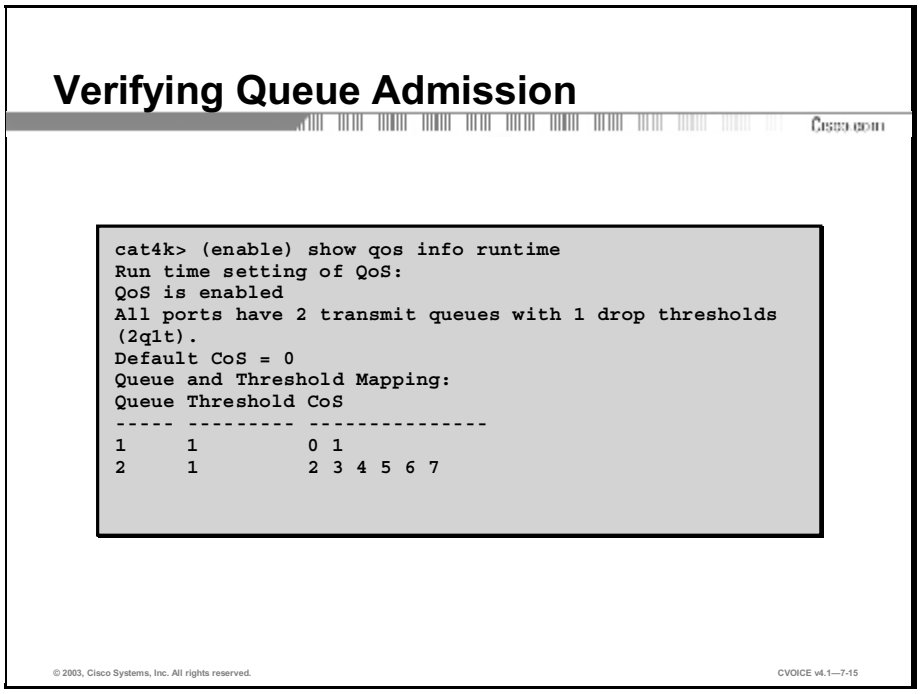
The addition of the Policy Feature Card (PFC) daughter card means that the Catalyst 6000 is capable of handling Layer 2, 3, and 4 QoS issues. You can use the PFC to enable advanced QoS tools, such as packet classification and marking, scheduling, and congestion avoidance, based on either Layer 2, Layer 3, or Layer 4 header information. You can configure multiple receive and transmit queues with thresholds and use them according to the QoS policy rules that are configured in the switch.

Configuration Examples

This topic illustrates configuration examples for QoS in the campus network.

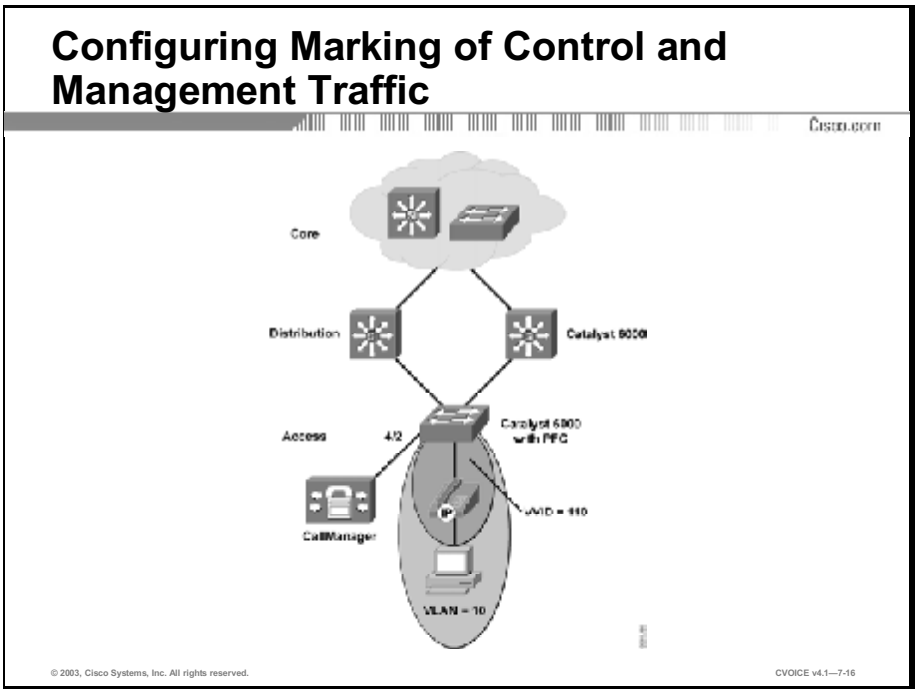


By default, only one queue is enabled on the Catalyst 4000 line of switches. Use the **set qos map** commands to enable the use of the second queue in CatOS Release 5.5.1. VoIP Control (CoS=3) frames should be placed into the second queue in the Catalyst 4000. These maps must be configured in pairs of CoS values, because the Catalyst 4000 examines the first two CoS bits only.

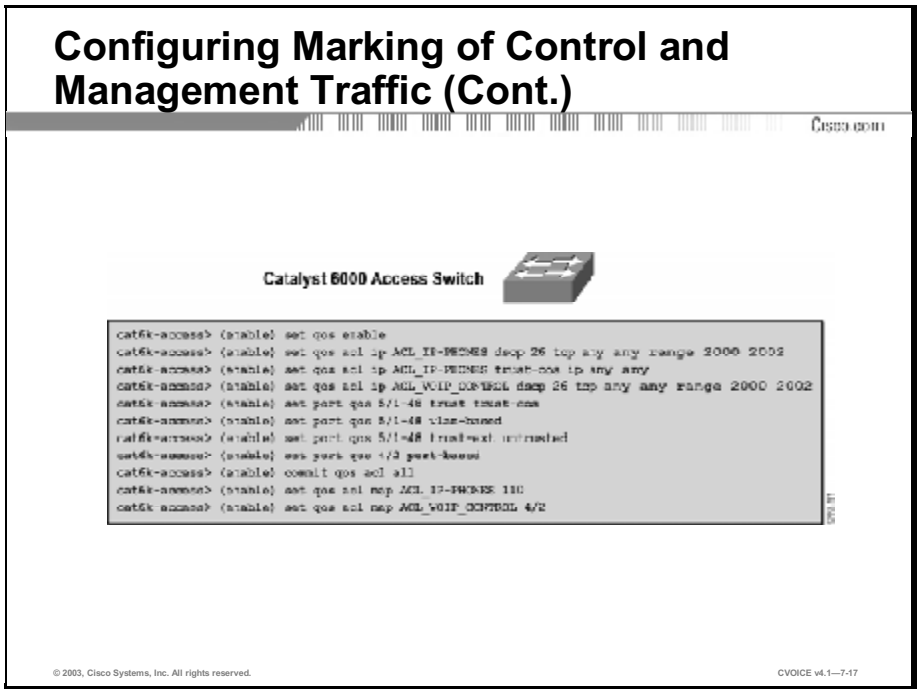


Output in this figure shows verification of the queue admission configuration.

Configuring Marking of Control and Management Traffic



To demonstrate marking of control and management traffic, you must assume that the access switch is a Catalyst 6000. The VVID is 110 and the data VLAN is 10. Assume also that the network is using the Skinny Client Control Protocol (SCCP) and that the Cisco CallManager is on port 4/2.



The commands in the figure show an example configuration for the network.

Cisco CallManager communicates with Cisco IP Phones and gateways using TCP ports 2000 to 2002. The following sample commands classify all Skinny protocol traffic from Cisco IP Phones and gateways (VLAN 110) and Cisco CallManager (4/2) as Differentiated Services (DiffServ) Code Point (DSCP) 26:

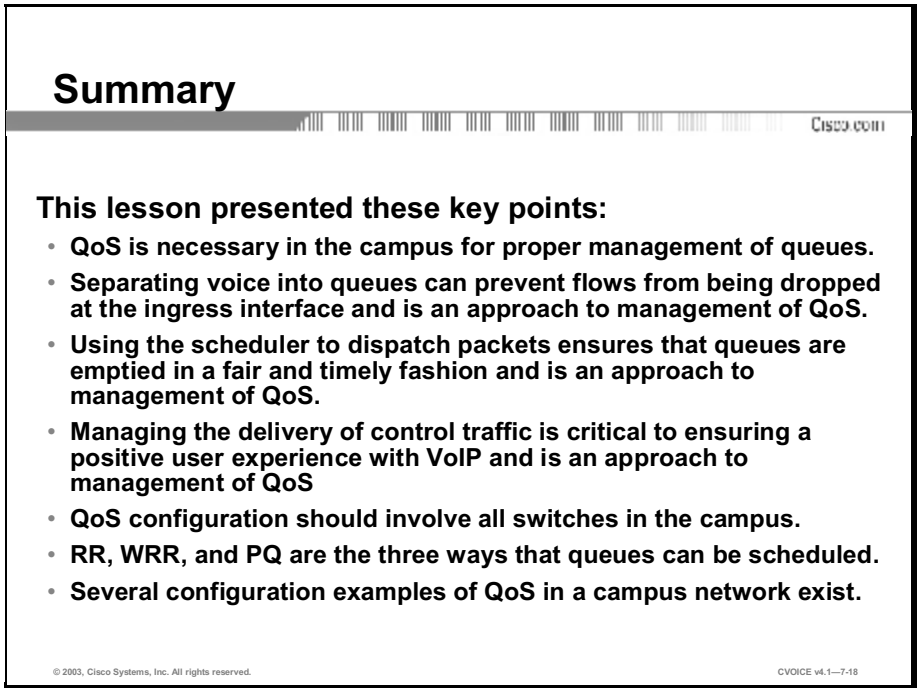
1. Enable switch-wide QoS.
2. Create an ACL (**ACL_IP-PHONES**), marking all Skinny client and gateway protocol traffic from the IP Phones and from Skinny protocol gateways with a DSCP value of 26 (AF31).
3. Add to the ACL_IP-PHONE access list, trusting all DSCP markings from the IP phone, so that the type of service (ToS)=5 RTP traffic is not rewritten.
4. Create an ACL (**ACL_VOIP_CONTROL**), marking all Skinny client and gateway protocol traffic from Cisco CallManager with a DSCP value of 26 (AF31).
5. Accept incoming Layer 2 CoS classification. (Current 10/100 version 1 line cards must have **trust-cos** enabled even though the parser returns an error.)
6. Configure the port so that all QoS associated with the port will be implemented on a VLAN basis.
7. Instruct the Cisco IP Phone to rewrite CoS from the PC to CoS=0 within the IP Phone Ethernet ASIC.
8. Inform Cisco CallManager port 4/2 that all QoS associated with the port will be done on a port basis.

9. Write the ACL to hardware.
10. Map the **ACL_IP-PHONE** ACL to the auxiliary VLAN.
11. Map the **ACL_VOIP_CONTROL** ACL to the Cisco CallManager port.

Note	Beginning with Release 3.0(5), Cisco CallManager includes the ability to configure the CoS values for all VoIP control and management traffic from Cisco CallManager, the IP Phones, and the Skinny protocol gateways (this does not include the AT and AS model analog gateways). This user-configurable classification means that network element access lists are no longer required for marking Skinny protocol VoIP control traffic. H.323 and Media Gateway Control Protocol (MGCP) traffic still require external network element marking.

Summary

This topic summarized the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Applying Quality of Service in the Campus
- Applying Quality of Service in the WAN lesson

References

For additional information, refer to these resources:

- "Designing a Campus" http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/avvidqos/qoscamps.htm
- "Cisco 'Deploying Quality of Service' (DQoS) course"

Quiz: Applying Quality of Service in the Campus

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Identify the areas of a campus network that require QoS services
- Describe separation of queues as an approach to QoS management in a campus network
- Describe queue scheduling as an approach to QoS management in a campus network.
- Describe marking control and management traffic as an approach to QoS management in a campus network.
- Provide an example of a QoS configuration on a campus network
- Describe three queuing and scheduling methods
- Configure switch-wide queuing and mark control and management traffic in a campus network

Instructions

Answer these questions.

Q1) Which ports connect to access switches and core switches?

A) access ports

B) core ports

C) distribution ports

D) fast ports

Q2) What is the result of voice packet loss?

A) clipping and skips

B) echo

C) jitter

D) overlap

Q3) Which QoS service is best for high-speed campus networks?

A) fair queuing

B) queue scheduling

C) separation of queues

D) marking control and management traffic

Q4) Before you enable multiple queues on Catalyst switches, you must make sure that _____ is disabled.

A) flow control

B) signaling

C) priority queuing

D) streaming

Q5) Which type of queue scheduling provides QoS by assigning bandwidth to higher priority applications?

A) priority queue

B) interleaving

C) round robin

D) weighted round-robin

Q6) Which queue scheduling method is best suited for branch office and wiring closet switches?

A) interleaving

B) round robin

C) weighted round-robin

D) priority queue

Q7) What is used to mark control and management traffic on Catalyst 3500 and 4000 switches that are enabled for Layers 3 and 4?

A) transmission control protocols

B) access control lists

C) signaling protocols

D) firewalls

Q8) What network problems adversely affect signaling traffic for gateways and telephones?

A) echo

B) congestion

C) delay and loss

D) network speed

Q9) Which strategy can you use to allow a large number of telephones on a network that does not have enough IP addresses?

A) disabling routing on the network

B) configuring stub areas

C) using Class C addressing only

D) isolating the telephones on an auxiliary VLAN

Q10) Which category of QoS is not suited for a campus network?

A) separation of queues

B) link efficiency

C) queue scheduling

D) marking control and management traffic

Q11) What is the recommended configuration for the receive interface in switch-wide queuing?

A) 2Q1T

B) 802.1p CoS

C) one standard FIFO queue

D) multiple receive and transmit queues with thresholds

Q12) What type of configuration can be used for queuing with Catalyst 6000 switches?

A) 2Q1T

B) 802.1p CoS

C) one standard FIFO queue

D) multiple receive and transmit queues with thresholds

Q13) Which command can be used to enable a second queue on the Catalyst 4000 series switches?

A) **set qos**

B) **set qos queue 2**

C) **set qos map**

D) **set qos 0-1**

Q14) Which command is used to enable switch-wide queuing?

A) **set qos enable**

B) **enable set qos**

C) **qos set enable**

D) **qos enable set**

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Applying Quality of Service in the WAN

Overview

This lesson introduces the need for quality of service (QoS) in a WAN, describes some of the tools that can be applied, and illustrates the configuration examples for the tools.

Importance

As Voice over IP (VoIP) networks grow to encompass the geographical areas served by WANs, it is essential that network administrators are able to apply QoS tools to the WAN.

Objectives

Upon completing this lesson, you will be able to:

- Describe six reasons for implementing QoS in a WAN
- List five QoS mechanisms that are used in a WAN
- Describe how bandwidth provisioning provides QoS in a WAN
- Illustrate how optimized queuing provides QoS in a WAN
- Describe how IP precedence and differentiated services code point provide link efficiency in a WAN
- List three link fragmentation and interleaving techniques that provide QoS in a WAN
- Identify the types of links that require traffic shaping

- Describe how Call Admission Control provides QoS in a WAN
- List five major components of QoS in a VoIP over Frame Relay network and describe three of those components
- List four major components of QoS in a VoIP over PPP network and describe one of those components
- Configure all QoS components on a VoIP over Frame Relay network using map classes and policies on the router
- Configure all QoS components on a VoIP over PPP network using map classes and policies on the router
- Describe the basics of QoS Policy Manager as a management tool for QoS

Learner Skills and Knowledge

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

- Knowledge of WAN technologies
- Knowledge of TCP/IP
- Basic knowledge of IP telephony

Outline

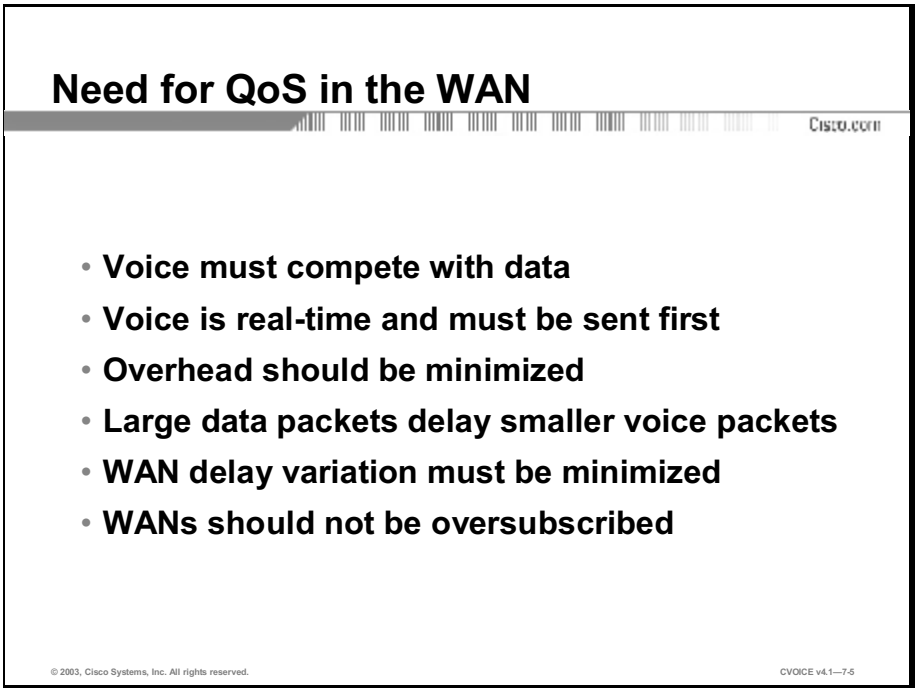
This lesson includes these topics:

- Overview
- Need for QoS on WAN Links
- Recommendations for Generic QoS in the WAN
- Bandwidth Provisioning
- Optimized Queuing
- Link Efficiency
- Link Fragmentation and Interleaving
- Traffic Shaping
- Call Admission Control

- QoS Recommendations for VoIP over Frame Relay
- QoS Recommendations for VoIP over PPP
- VoIP over Frame Relay Configuration
- VoIP over PPP Configuration
- CiscoWorks QPM for QoS
- Summary
- Assessment (Quiz): Applying Quality of Service in the WAN
- Assessment (Complex Lab): Lab Exercise 7-1

Need for QoS on WAN Links

This topic defines the need for quality of service (QoS) in a WAN.



You must consider and implement certain QoS measure before voice can be placed on a WAN to ensure the proper performance of voice and data applications. The following factors explain the need for QoS:

- **Voice must compete with data:** Voice traffic demand on the WAN is typically smooth; each voice call consumes a relatively fixed amount of bandwidth for the duration of the call. On the other hand, data traffic is bursty, peaking and leveling off based on user access. The amount of total bandwidth that you provision must have the capacity to carry all of the expected traffic.

- **Voice is real time and must be sent first:** Because voice is a real-time application and delayed packets have a severe impact on performance, you must prioritize voice ahead of data traffic that is not real-time traffic.

- **Overhead should be minimized:** Voice is sent using User Datagram Protocol (UDP). Unfortunately, this requirement adds significant overhead to the overall packet size. You must identify a means for numbering the packets that are needed because minimizing the overhead with compression allows for smaller, more efficient packets.

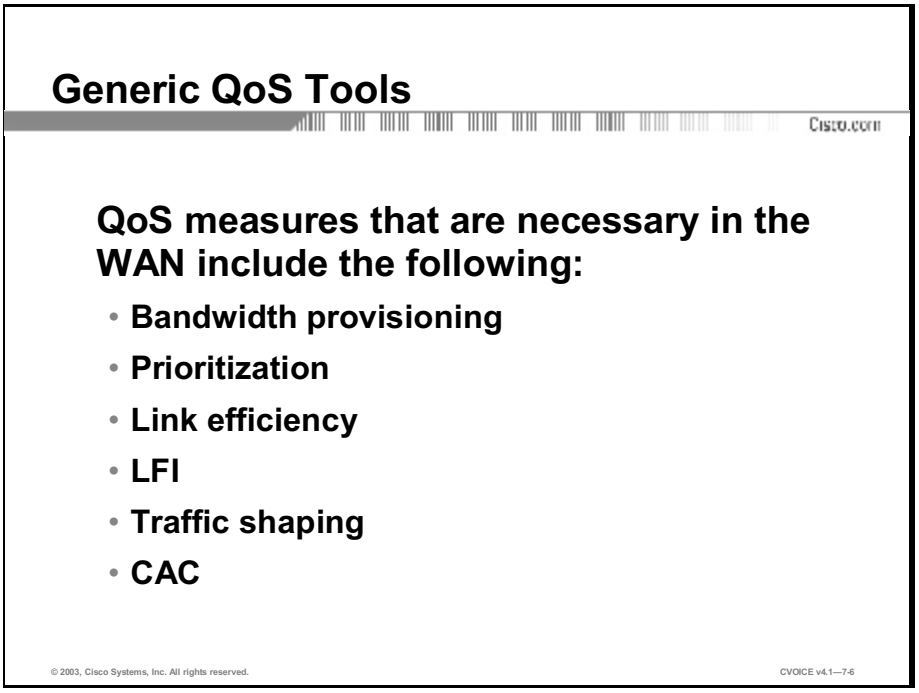
- **Large data packets delay smaller voice packets:** With certain applications such as file transfers and web browsing, data packets that compete with voice can be relatively large. Voice packets are forced to wait until the larger data packets are sent. By fragmenting the data packets into smaller, more manageable sizes, you can reduce the delay that is experienced by voice packets.

- **WAN delay variation must be minimized:** The natural behavior of certain WAN technologies, such as Frame Relay, ATM, and PPP, can exacerbate delay variation and result in poor voice performance. By using tools to reduce the delay variation on WAN technologies, you can add significant performance to voice applications.

- **WANs should not be oversubscribed:** If you place too many voice calls on a WAN, the necessary bandwidth that is required by data applications will be choked. You must take care to ensure that data still gets its deserved bandwidth. Excess voice calls can severely impact all calls on the network.

Recommendations for Generic QoS in the WAN

This topic lists generic QoS tools.

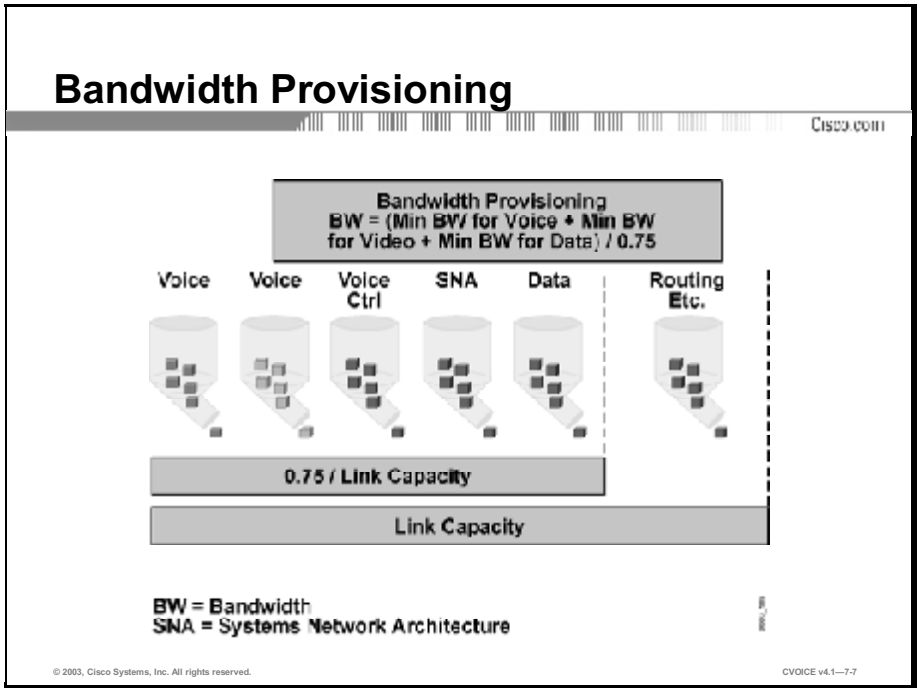


Depending on the Layer 2 technology that you use, the following QoS measures may be necessary in the WAN:

- Bandwidth provisioning
- Prioritization
- Link efficiency
- Link fragmentation and interleaving (LFI)
- Traffic shaping
- Call Admission Control (CAC)

Bandwidth Provisioning

This topic describes bandwidth provisioning as a tool for implementing QoS in the WAN.

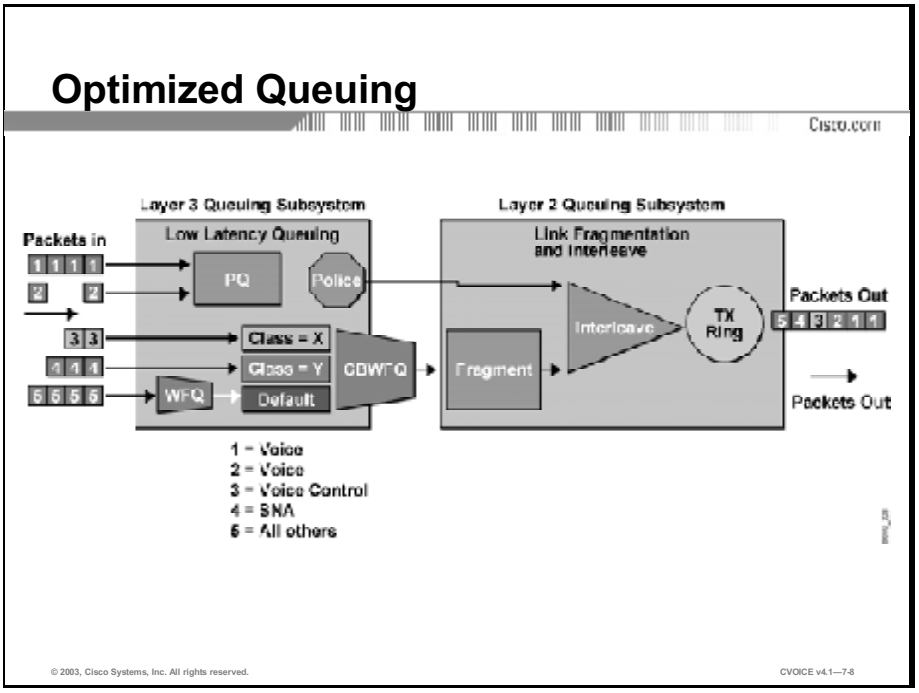


The figure represents a typical network. This network has a number of delay-sensitive traffic types: voice, video, and Systems Network Architecture (SNA). Before you place voice and video on a network, you must ensure that adequate bandwidth exists for all required applications. SNA is also delay-sensitive but should not be queued *ahead* of voice and video.

To begin, the minimum bandwidth requirements for each major application (for example, voice media streams, video streams, voice control protocols, and all data traffic) should be summed. This sum represents the minimum bandwidth requirement for any given link, and it should consume no more than 75 percent of the total bandwidth that is available on that link. This 75 percent rule assumes that some bandwidth is required for overhead traffic, such as routing and Layer 2 keepalives, as well as for additional applications such as e-mail, HTTP traffic, and other data traffic that is not easily measured.

Optimized Queuing

This topic describes optimized queuing as a tool for implementing QoS in the WAN.



When you are choosing from among the many available prioritization schemes, the major factors that you must consider include the type of traffic on the network and the wide area media that is being traversed.

For multiservice traffic over an IP WAN, Cisco Systems recommends Low Latency Queuing (LLQ) for low-speed links. This approach allows up to 64 traffic classes with the ability to specify, for example, priority queuing (PQ) behavior for voice and interactive video, a minimum bandwidth for SNA data and market data feeds, and as illustrated in the figure, weighted fair queuing (WFQ) to other traffic types. The requirements are as follows:

- Voice is placed into a queue with PQ capabilities and allocated a bandwidth of 48 kbps. The entrance criterion to this queue should be the differentiated services code point (DSCP) value of Express Forwarding (EF), or IP precedence value of 5. Traffic in excess of 48 kbps is dropped if the interface becomes congested. Therefore, you must use an admission control mechanism to ensure that you do not exceed this value.

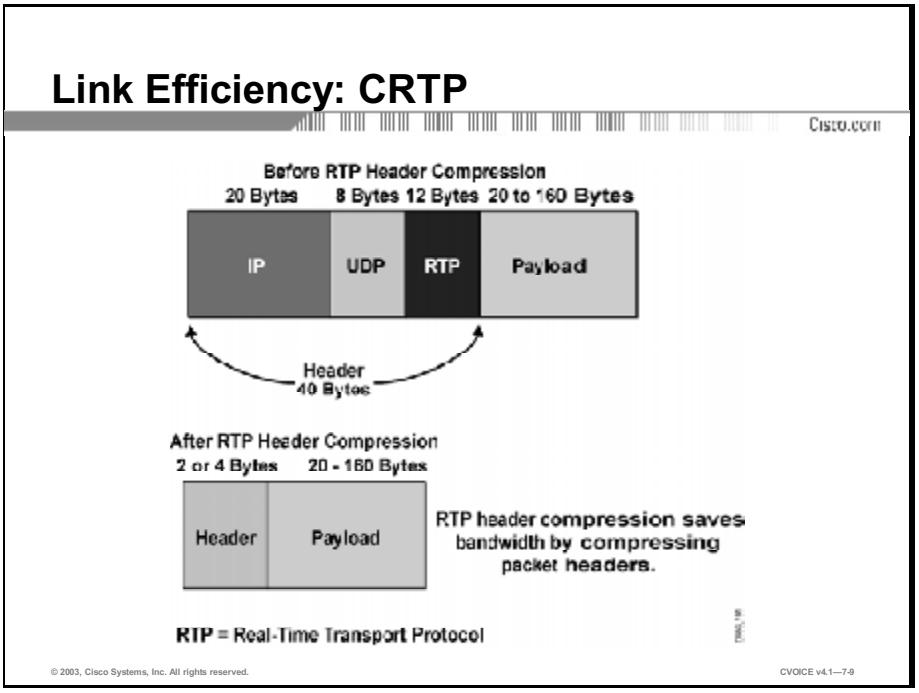
- As the WAN links become congested, it is possible to completely starve the voice control signaling protocols, eliminating the capacity of the IP Phones to complete calls across the IP WAN. Voice control protocol traffic, such as H.323 and the Skinny Client Control Protocol (SCCP), requires its own class-based weighted fair queuing (CBWFQ) with a minimum configurable bandwidth equal to a DSCP value of AF31, which correlates to an IP precedence value of 3.

- SNA traffic is placed into a queue that has a specified bandwidth of 56 kbps. Queuing operation within this class is FIFO with a minimum allocated bandwidth of 56 kbps. Traffic in this class that exceeds 56 kbps is placed in the default queue. The entrance criterion to this queue could be TCP port numbers, a Layer 3 address, IP precedence, or a DSCP.

- You can place all remaining traffic in a default queue. If a bandwidth is specified, the queuing operation is FIFO. Alternatively, specifying the keyword **fair** assigns WFQ to the operation.

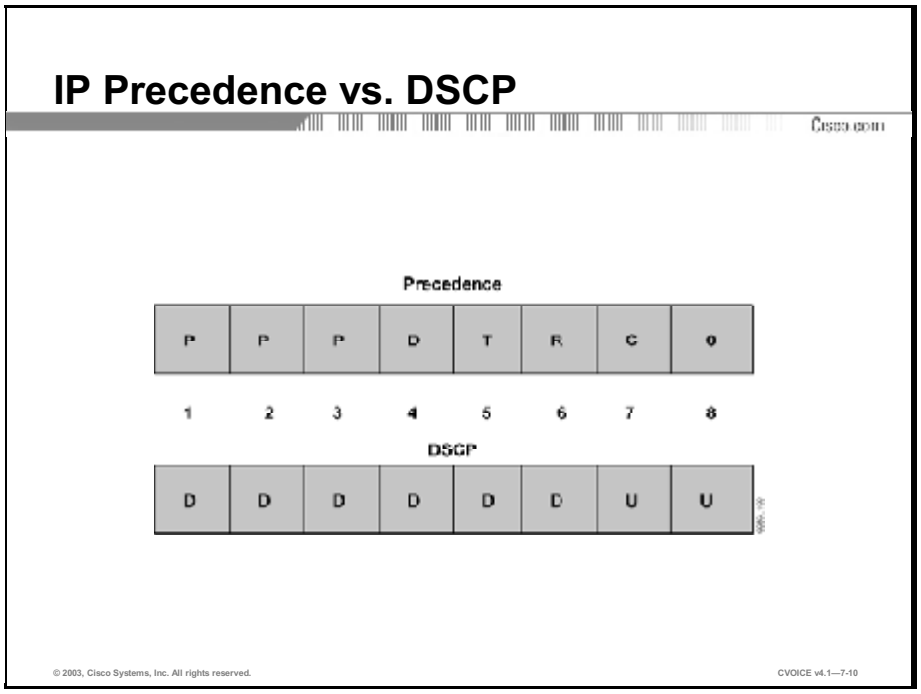
Link Efficiency

This topic describes link efficiency as a tool for implementing QoS in the WAN.



Because wide-area bandwidth is often prohibitively expensive, only low-speed circuits may be available or cost-effective when you are interconnecting remote sites. In this scenario it is important to achieve the maximum savings by transmitting as many voice calls as possible over the low-speed link. Many compression schemes, such as G.729, can squeeze a 64-kbps call down to an 8-kbps payload. Cisco gateways and IP Phones support a range of coder-decoders (codecs) that enhance efficiency on these low-speed links.

The link efficiency is further increased by using Compressed RTP (CRTP), which compresses a 40-byte IP + UDP + RTP header to approximately 2 to 4 bytes. In addition, voice activity detection (VAD) takes advantage of the fact that in most conversations, only one party is talking at a time. VAD recovers this empty time and allows data to use the bandwidth.



IP Precedence

The 8-bit class of service (CoS) field in an IP packet header was originally defined in RFC 791 (superseded by RFC 1122). It defined the most significant bits as shown in the table.

Table 1: IP Precedence

Binary Value	Precedence Value	Description
111	7	Network Control
110	6	Internetwork Control
101	5	Critical
100	4	Flash Override
011	3	Flash
010	2	Immediate
001	1	Priority
000	0	Routine

In addition, the next 4 bits, when turned on, refer to the following:

- **Bit 4, D:** Instructs the network to minimize delay
- **Bit 5, T:** Instructs the network to maximize throughput
- **Bit 6, R:** Instructs the network to maximize reliability
- **Bit 7, C:** Instructs the network to minimize costs
- **Bit 8:** Is reserved for future use

DSCP

The newest use of the eight CoS bits is commonly called the Differentiated Services (DiffServ) standard. It uses the same precedence bits (the most significant bits—1, 2, and 3) for priority setting, but further clarifies their functions and definitions and offers finer priority granularity through use of the next three bits in the CoS field. DiffServ reorganizes and renames the precedence levels (still defined by the three most significant bits of the CoS field) into the categories shown in the table.

Table 2: DiffServ Standard

Precedence Bits	Description
Precedence 7	Stays the same (link layer and routing protocol keepalive)
Precedence 6	Stays the same (used for IP routing protocols)
Precedence 5	EF
Precedence 4	Class 4
Precedence 3	Class 3
Precedence 2	Class 2
Precedence 1	Class 1
Precedence 0	Best effort

Bits 3 and 4 of the CoS field (now called the DSCP in the DiffServ standard) allow further priority granularity through the specification of packet drop probability for any of the defined classes. Collectively, classes 1 through 4 are referred to as Assured Forwarding (AF). The table illustrates the DSCP coding for specifying the priority level (class) plus the drop percentage. (Bits 1, 2, and 3 define the class; bits 4 and 5 specify the drop percentage; bit 6 is always 0.) As an example, AF41 is expressed as 100010, where the first three bits represent class 4, the next two bits specify a low drop percentage, and the last bit is always 0. AF41 has a higher priority than any class 3, 2, or 1, and enjoys the lowest drop percentage.

Table 3: DSCP Coding

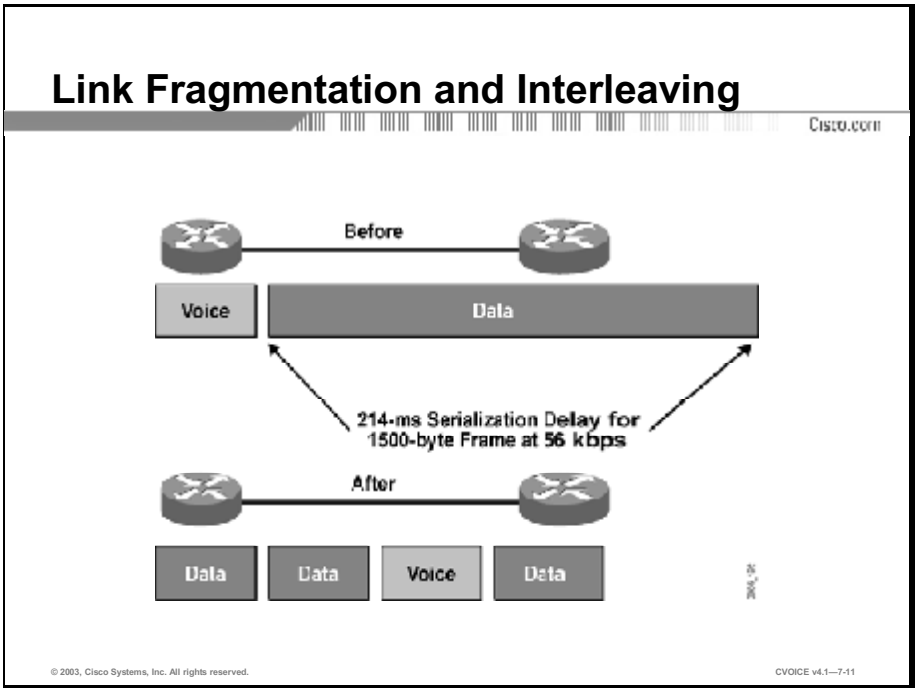
Drop Percentage	DSCP Coding			
	Class 1	Class 2	Class 3	Class 4
Low drop percentage	001010	010010	011010	100010
Medium drop percentage	001100	010100	011100	100100
High drop percentage	001110	010110	011110	100110

Using this system, a device first prioritizes traffic by class, then differentiates and prioritizes traffic that is in the same class by considering the drop percentage. It is important to note that this standard does not offer a precise definition of low, medium, and high drop percentages. Additionally, not all devices recognize the DiffServ bit 4 and 5 settings. In fact, even when the settings are recognized, they do not necessarily trigger the same forwarding action from each device on the network.

Each device implements its own response in relation to the packet priorities that it detects. The DiffServ proposal is meant to allow a finer granularity of priority setting for the applications and devices that can use it, but it does not specify interpretation (that is, action to be taken). In this application, bits 7 and 8 are unused.

Link Fragmentation and Interleaving

This topic describes LFI as tool for implementing QoS in the WAN.

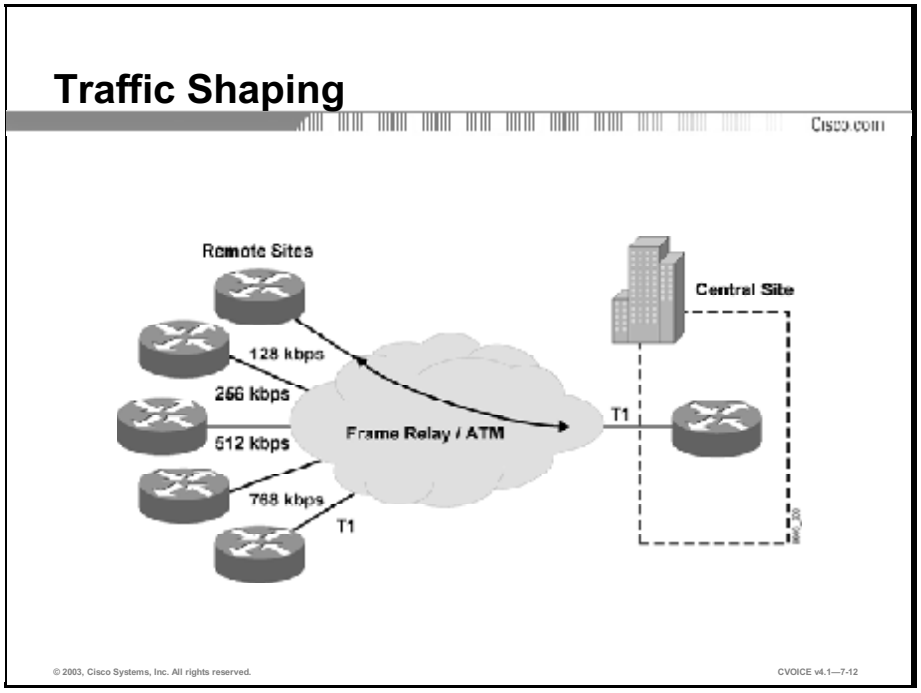


For low-speed links (less than 768 kbps), it is necessary to use techniques that provide LFI. This approach places bounds on jitter by preventing the delay of voice traffic behind large data frames. The following three techniques exist for this purpose:

- Multilink PPP (MLP) for point-to-point serial links
- FRF.12 (Frame Relay Fragmentation) for Frame Relay
- MLP over ATM for ATM connections

Traffic Shaping

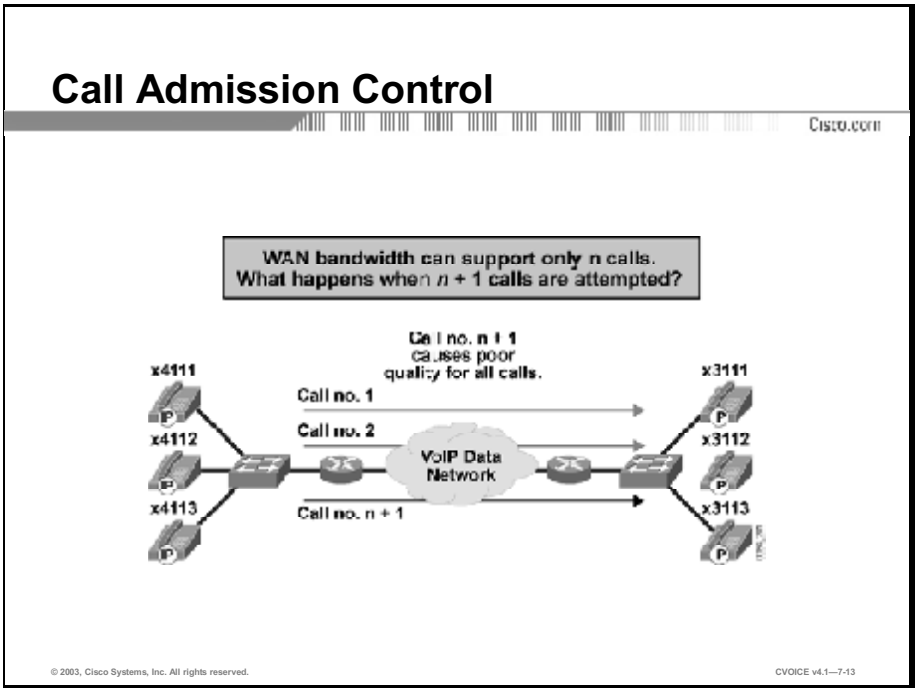
This topic describes traffic shaping as a tool for implementing QoS in the WAN.



Traffic shaping is required for multiple-access nonbroadcast media, such as ATM and Frame Relay, where the physical access speed varies between two endpoints. Traffic-shaping technology accommodates mismatched access speeds. In the case of Frame Relay with FRF.12, traffic shaping also allows delay variation, or jitter, to be bounded appropriately.

Call Admission Control

This topic describes CAC as a tool for implementing QoS in the WAN.

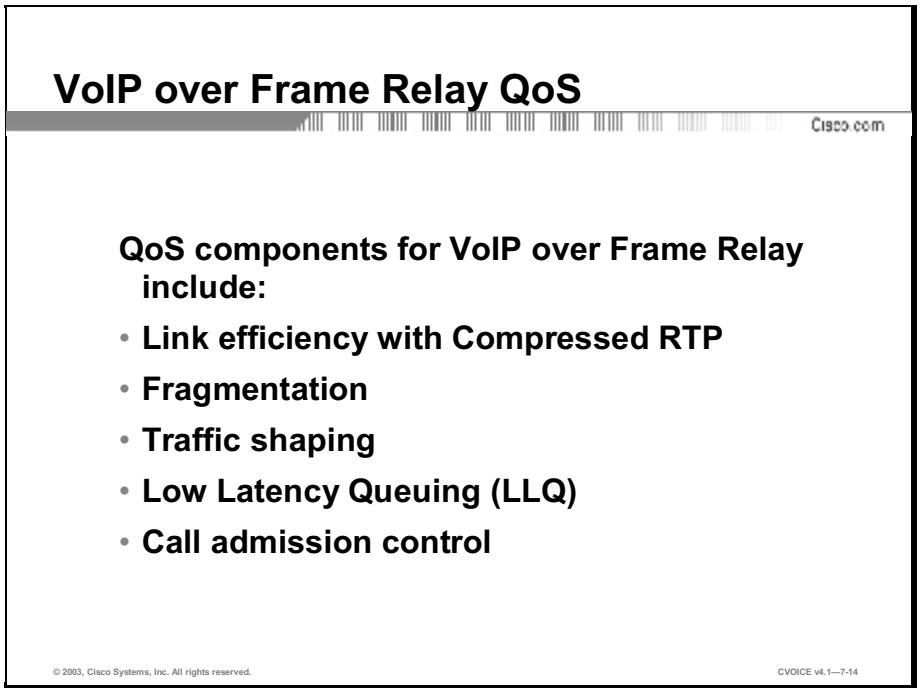


CAC is required to ensure that network resources are not oversubscribed. CAC could be described as a way to protect *voice from voice*. Calls that exceed the specified bandwidth are either rerouted using an alternative route such as the public switched telephone network (PSTN), or a busy tone is returned to the calling party. This way the next voice call does not degrade the quality of all the calls on the link. You can implement CAC on a gatekeeper or throughout the network by using Cisco CallManager.

Reference For more information on VoIP CAC, see the following topic on the Cisco.com website: http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/cac.htm

QoS Recommendations for VoIP over Frame Relay

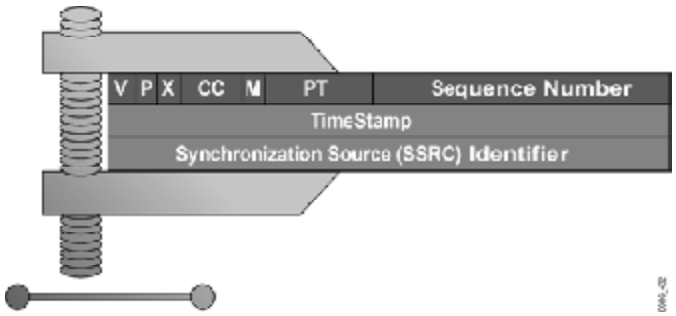
This topic identifies some of the QoS tools implemented in a Frame Relay network to support VoIP.



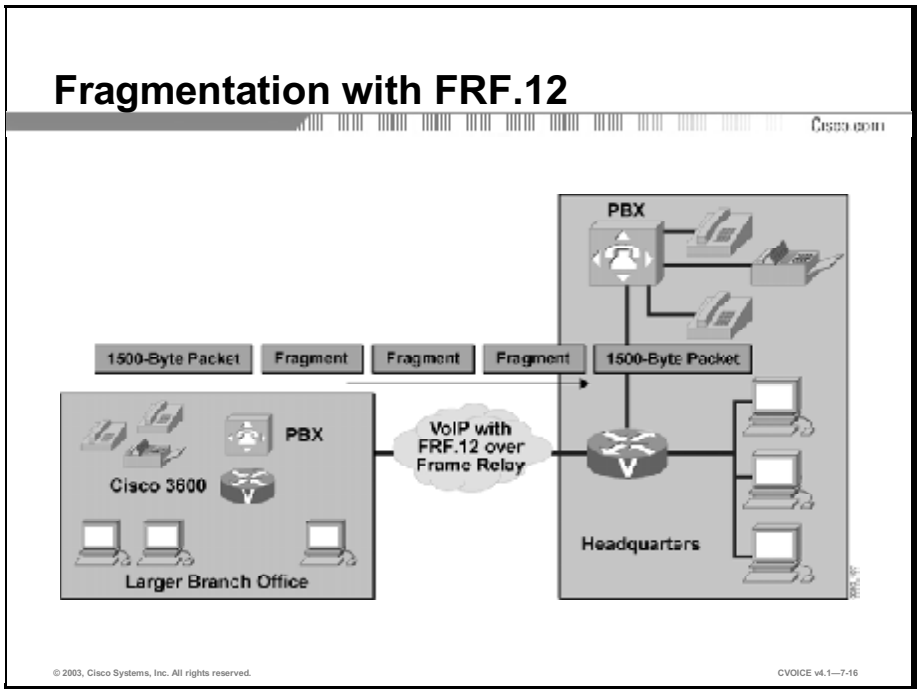
The five major components of QoS that are particular to VoIP over Frame Relay are as follows:

- Link efficiency with CRTP
- Fragmentation
- Traffic shaping
- LLQ
- CAC

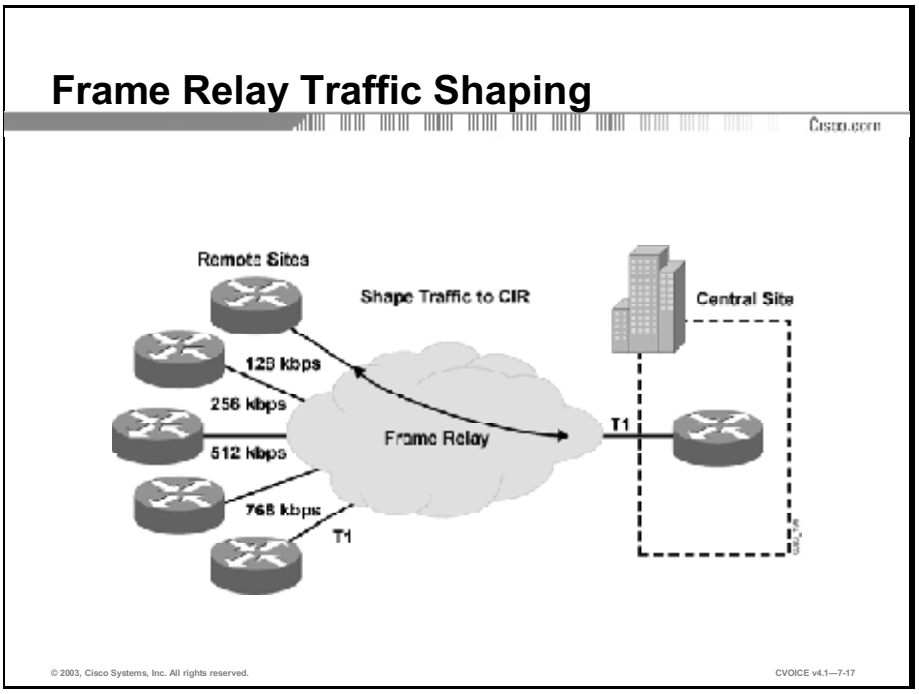
Link Efficiency for Frame Relay



CRTP is explicitly enabled on a Frame Relay interface. Compressing the RTP header can reduce it from 40 bytes to 2 or 4 bytes, depending on whether the cyclic redundancy check (CRC) is included.



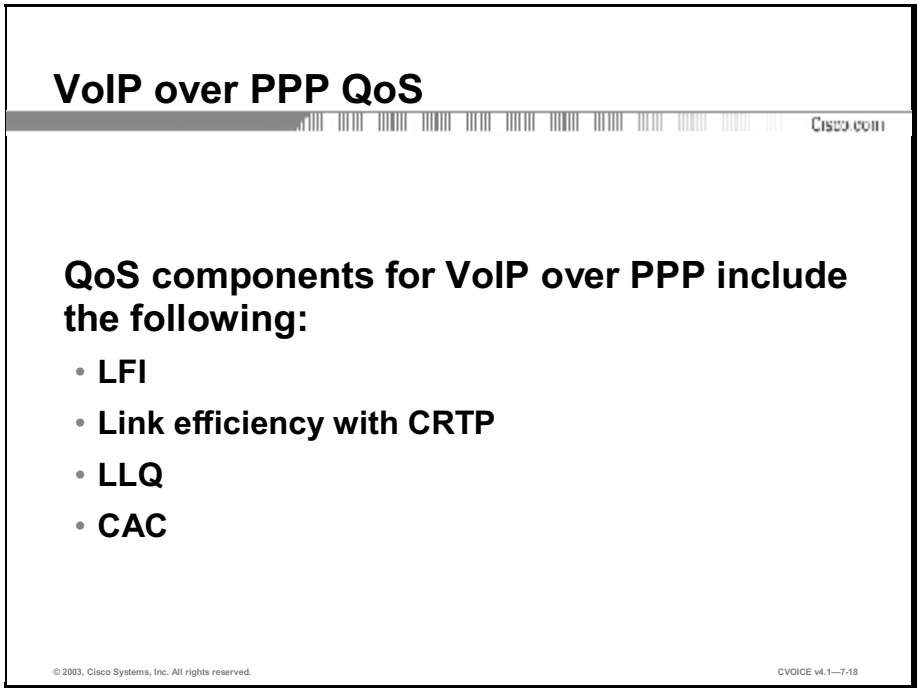
When running VoIP over Frame Relay, you must facilitate fragmentation of larger data frames to allow interleaving of smaller voice frames. This fragmentation is accomplished with FRF.12. FRF.12 adds an extended header to the Frame Relay frame that identifies the frame as fragmented and indicates a sequence number for reassembly. It provides end-to-end fragmentation on a per-virtual circuit (VC) basis. As stated earlier, fragmentation is necessary only on links of 768 kbps or less.



You must enable Frame Relay traffic shaping to shape the VC to committed information rate (CIR) value. Shaping to the CIR for each VC that carries voice ensures that the service provider does not mark any voice frames discard eligible (DE). Frame Relay traffic shaping (FRTS) provides useful parameters for managing network traffic congestion on Frame Relay networks. FRTS eliminates bottlenecks in Frame Relay networks with high-speed connections to the central site, and low-speed connections to the branch sites. FRTS ensures that traffic above the CIR on the link is not dropped, but is buffered and sent when there is capacity on the link. You can configure rate enforcement values to limit the rate at which data is sent from the VC at the central site. Without traffic shaping, certain virtual circuits may overuse the outbound interface, "starving" other VCs and causing delay and jitter.

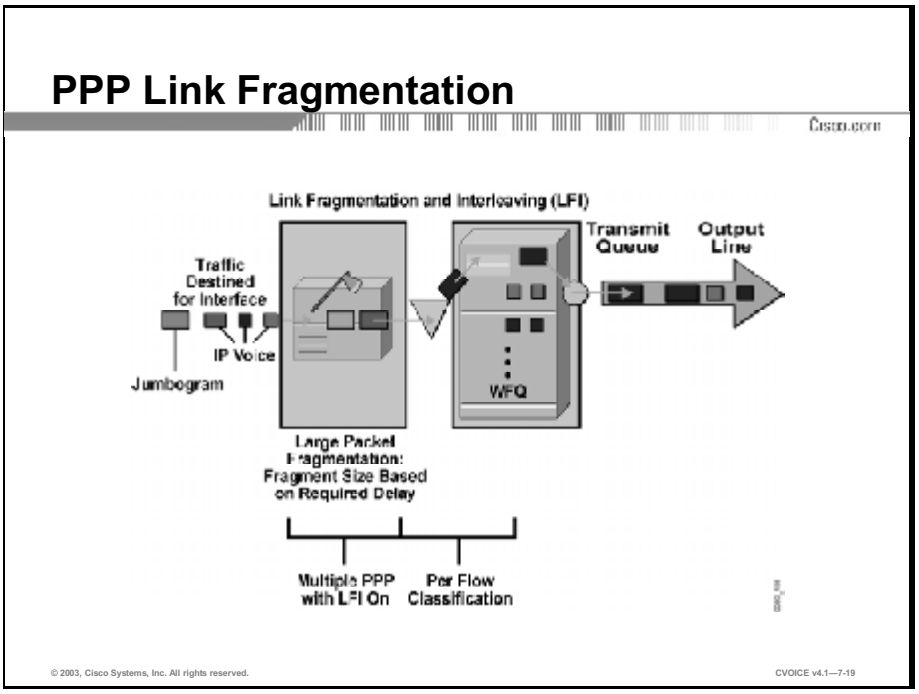
QoS Recommendations for VoIP over PPP

This topic identifies some of the QoS tools implemented in a PPP network to support VoIP.



Following are the four major components of QoS that are particular to VoIP over PPP:

- LFI
- Link efficiency with CRTP
- LLQ
- CAC



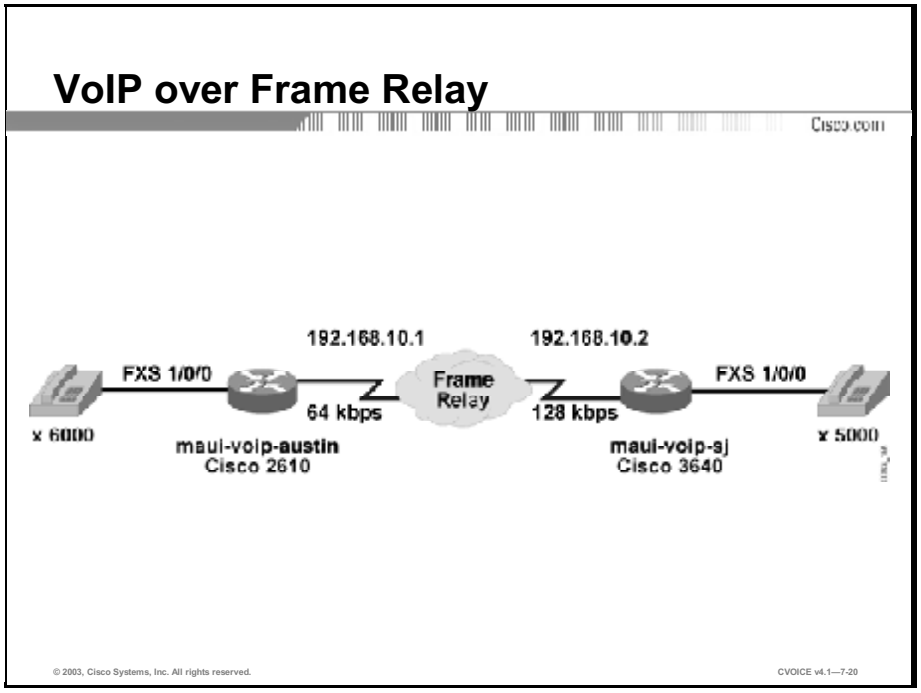
While 1500 bytes is a common size for data packets, a typical VoIP packet (carrying G.729 voice frames) is approximately 66 bytes (20 bytes voice payload, 6 bytes Layer 2 header, 20 bytes RTP and UDP header, and 20 bytes IP header).

Now, imagine a 56-kbps leased-line link where voice and data traffic coexist. If a voice packet is ready to be serialized just when a data packet starts transmission over the link, a problem occurs. The delay-sensitive voice packet has to wait 214 ms before transmission (it takes 214 ms to serialize a 1500-byte packet over a 56-kbps link).

Large data packets can significantly delay delivery of small voice packets, reducing speech quality. Fragmenting these large data packets into smaller packets and interleaving voice packets among the fragments reduces delay and jitter. The Cisco IOS® LFI feature helps satisfy the real-time delivery requirements of VoIP. The figure illustrates the operation of LFI.

VoIP over Frame Relay Configuration

This topic includes configuration examples for Frame Relay QoS.



For this example, use the network shown in the figure. Assume that a customer wants to set up all components of QoS for a VoIP over Frame Relay network.

VoIP over Frame Relay QoS

Cisco.com

Access List Configuration

```
access-list 102 permit udp any any range 16384 32767
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
```

Notes: **access-list 102** matches VoIP traffic based on the UDP port range. Both odd and even ports are put into the PQ. **access-list 103** matches VoIP signaling protocol. In this case, H.323v2 is used with the Fast Start Feature.

VoIP over Frame Relay QoS (Cont.)

Cisco.com

Class Maps and Policy Maps Configuration

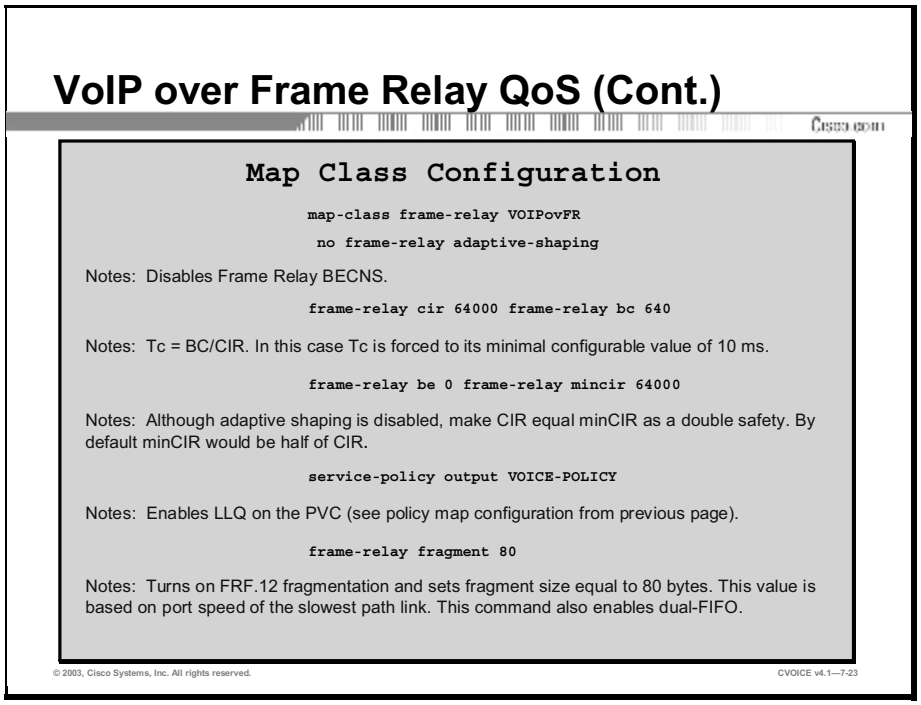
```
class-map match-all voice-signaling
 match access-group 103
class-map match-all voice-traffic
 match access-group 102
```

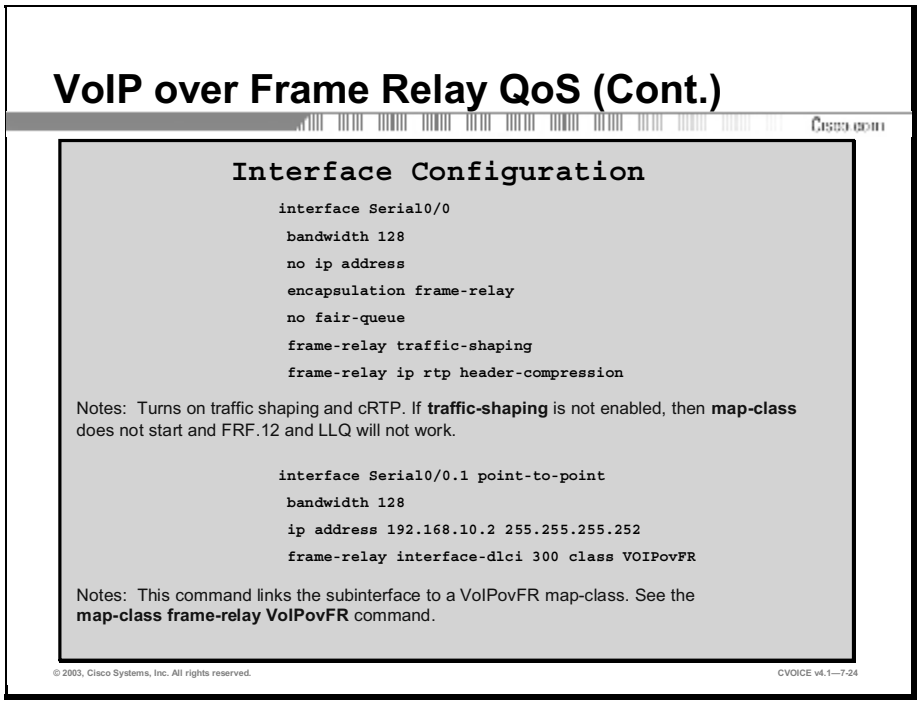
Notes: Definition of the voice-signaling and traffic class maps. **voice-traffic** class uses **access-list 102** for its matching criteria. **voice-signaling** class uses **access-list 103** for its matching criteria.

```
policy-map VOICE-POLICY
 class voice-traffic
  priority 45
 class voice-signaling
  bandwidth 8
class default-class
  fair-queue
```

Notes: The policy map defines how the link resources are assigned to the different map classes. In this configuration, strict PQ is assigned to the **voice-traffic** class with a maximum bandwidth of 45 kbps. This also assigns a queue for **voice-signaling** traffic that ensures 8 kbps. Note that this is optional and has nothing to do with good voice quality. Instead, it is a way to secure signaling.

These figures illustrate the commands used for implementing Frame Relay QoS using map classes and policies on the router.





These figures continue the QoS commands.

VoIP over Frame Relay QoS (Cont.)

Cisco.com

Dial-Peer Configuration—Precedence

```
dial-peer voice 1 pots
 destination-pattern 6000
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 5000
 session target ipv4:192.168.10.2
 ip precedence 5
```

Notes: Sets the precedence value to critical for systems that do not understand DSCP.

VoIP over Frame Relay QoS (Cont.)

Cisco.com

Dial-Peer Configuration—DSCP

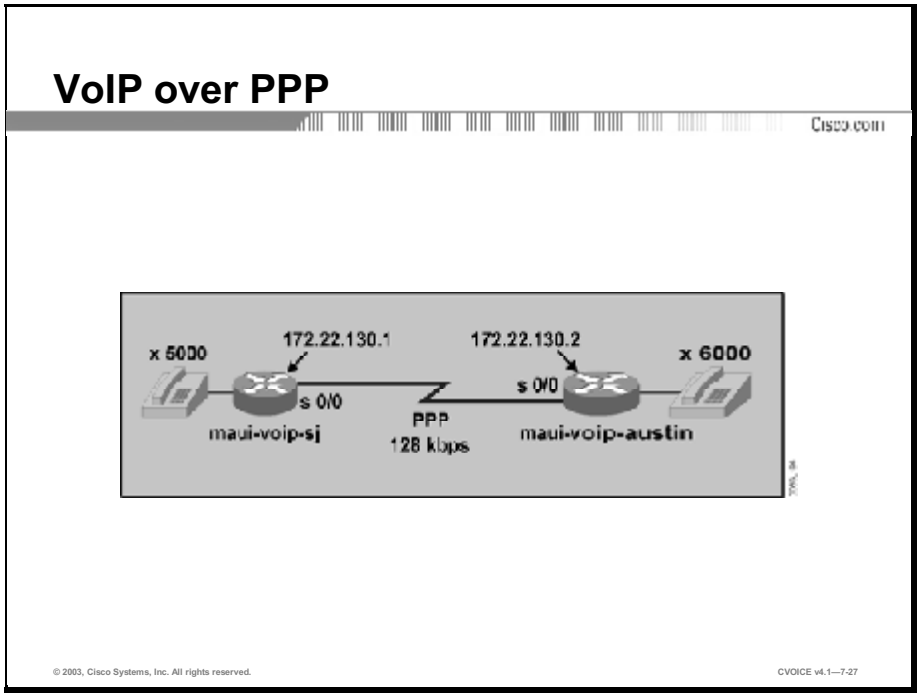
```
dial-peer voice 1 pots
 destination-pattern 6000
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 5000
 session target ipv4:192.168.10.2
 ip qos dscp ef media
```

Notes: Sets the DSCP value to Express Forward for systems that understand DSCP. The **media** term applies DSCP to media payload packets.

These figures continue the QoS commands.

VoIP over PPP Configuration

This topic includes configuration examples for VoIP over PPP.



For the next example, use the “VoIP over PPP” network displayed here. Assume that a customer wants to set up all components of QoS for a VoIP over PPP network.

VoIP over PPP QoS

Cisco.com

Access List Configuration

```
access-list 102 permit udp any any range 16384 37276
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
```

Notes: **access-list 102** matches VoIP traffic based on the UDP port range Both odd and even ports are put into the PQ. **access-list 103** is used to match VoIP signaling protocol. In this case we are using H.323v2 with Fast Start feature.

VoIP over PPP QoS (Cont.)

Cisco.com

Class Maps and Policy Maps Configuration

```
class-map match-all voice-signaling
 match access-group 103
class-map match-all voice-traffic
 match access-group 102
```

Notes: Definition of the voice-signaling and traffic class maps. **voice-traffic** class uses access-list 102 for its matching criteria. **voice-signaling** class uses access-list 103 for its matching criteria.

```
policy-map VOICE-POLICY
 class voice-traffic
  priority 45
 class voice-signaling
  bandwidth 8
class default-class
  fair-queue
```

Notes: The policy map defines how the link resources are assigned to the different map classes. In this configuration, strict PQ is assigned to the voice-traffic class with a maximum bandwidth of 45 kbps. This also assigns a queue for voice-signaling traffic that ensures 8 kbps. Note that this is optional and has nothing to do with good voice quality. Instead, it is a way to secure signaling.

These figures illustrate the commands that are used for implementing PPP QoS using the map classes and policies on the router.

VoIP over PPP QoS (Cont.)

Multilink Interface Configuration

Notes: MLP is strictly an LFI mechanism. It does not bundle multiple serial interfaces to the same virtual interface as the name suggests (This bundling is done for data and NOT recommended for voice). The end result may manifest itself as jitter and no audio.

```
interface Multilink1
 bandwidth 128
```

Notes: The bandwidth command needs to be set correctly for the right fragment size to be calculated.

```
ip address 172.22.130.1 255.255.255.252
 ip tcp header-compression iphc-format
 service-policy output VOICE-POLICY
```

Notes: Sets up LLQ, an outbound operation applied to the outbound WAN interface.

```
no cdp enable
 ppp multilink
 ppp multilink fragment-delay 10
```

Notes: The configured value of 10 sets the fragment size such that all fragments will have a 10ms maximum serialization delay.

```
ppp multilink interleave
multilink-group 1
```

Notes: This command links the multilink interface to the physical serial interface.

```
ip rtp header-compression
```


VoIP over PPP QoS (Cont.)

Interface Configuration

```
interface Serial0/0
 bandwidth 128
 no ip address
 encapsulation ppp
 clockrate 128000
 ppp multilink
 multilink-group 1
```

Notes: This command links the multilink interface to the physical serial interface.

These figures continue the QoS commands.

VoIP over PPP QoS (Cont.)

Cisco.com

Dial-peer Configuration—Precedence

```
dial-peer voice 1 pots
 destination-pattern 6000
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 5000
 session target ipv4:192.168.10.2
 ip precedence 5
```

Notes: Sets the precedence value to critical for systems that do not understand DSCP.

Or:

VoIP over PPP QoS (Cont.)

Cisco.com

Dial-peer Configuration—DSCP

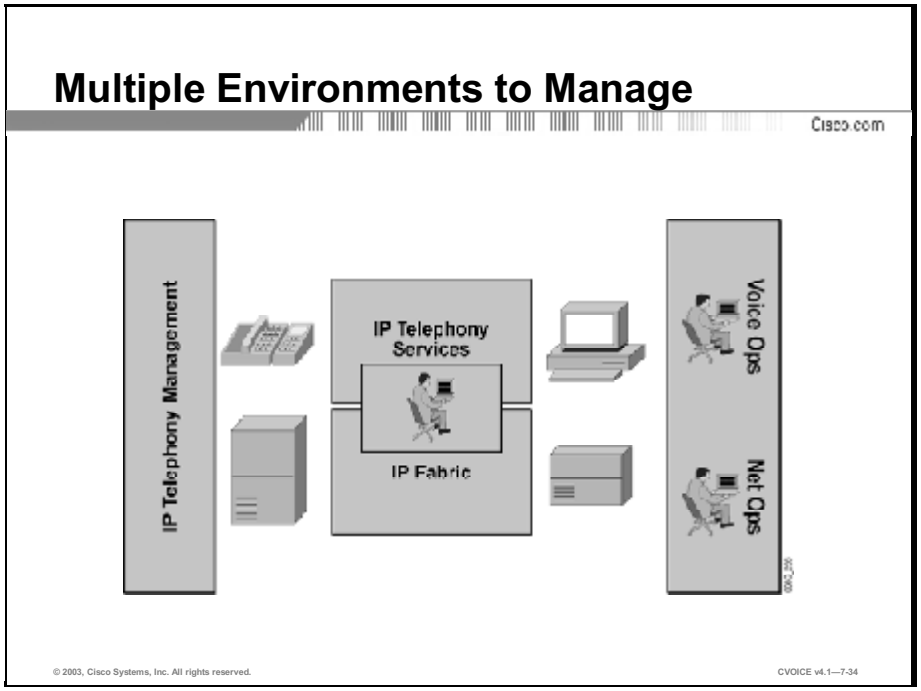
```
dial-peer voice 1 pots
 destination-pattern 6000
 port 1/0/0
!
dial-peer voice 2 voip
 destination-pattern 5000
 session target ipv4:192.168.10.2
 ip qos dscp ef media
```

Notes: Sets the DSCP value to Express Forward for systems that understand DSCP. The **media** term applies DSCP to media payload packets.

These figures illustrate the required configuration on dial peers.

CiscoWorks QPM for QoS

This topic describes the basics of CiscoWorks QoS Policy Manager (QPM) as a management tool for QoS.

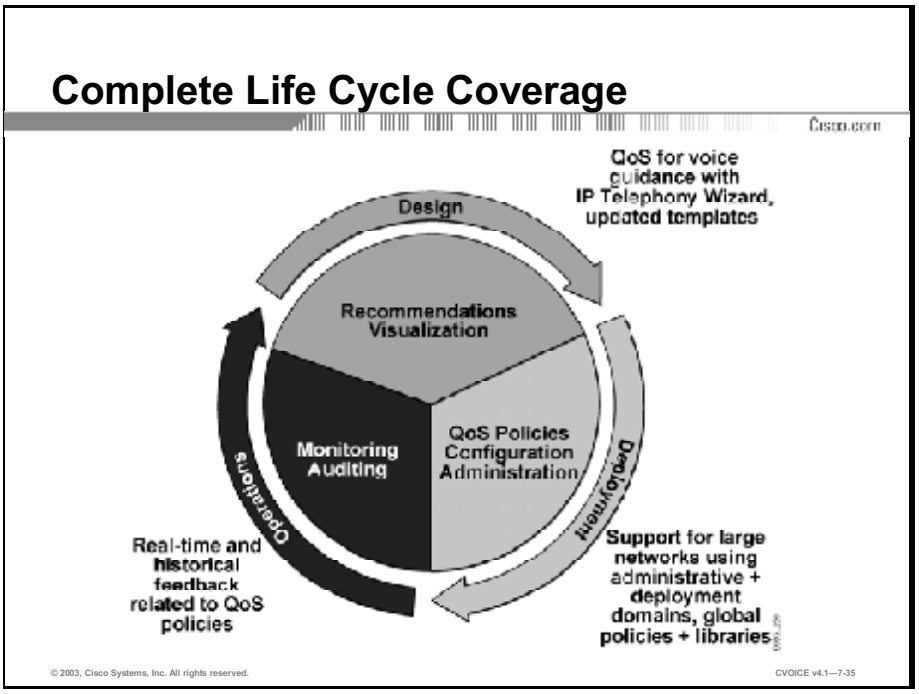


While the need for managing QoS in a voice-enabled environment is obvious, the configuration, deployment, and analysis of the requisite QoS policies may not be as intuitive.

The primary challenge for network managers is to consistently deploy policies in the devices that are located throughout a network to operate voice correctly. However, using the QoS features within intelligent network devices can be a complex exercise for network managers.

The sheer number of devices involved, coupled with the additional complexity of having different devices support different sets of QoS mechanisms, makes this a daunting task. To deploy these end-to-end intelligent services, network managers must use automated tools only. Without automated policy tools like QPM, it is highly likely that a user who tries to apply policies across a complex network will end up with inconsistencies.

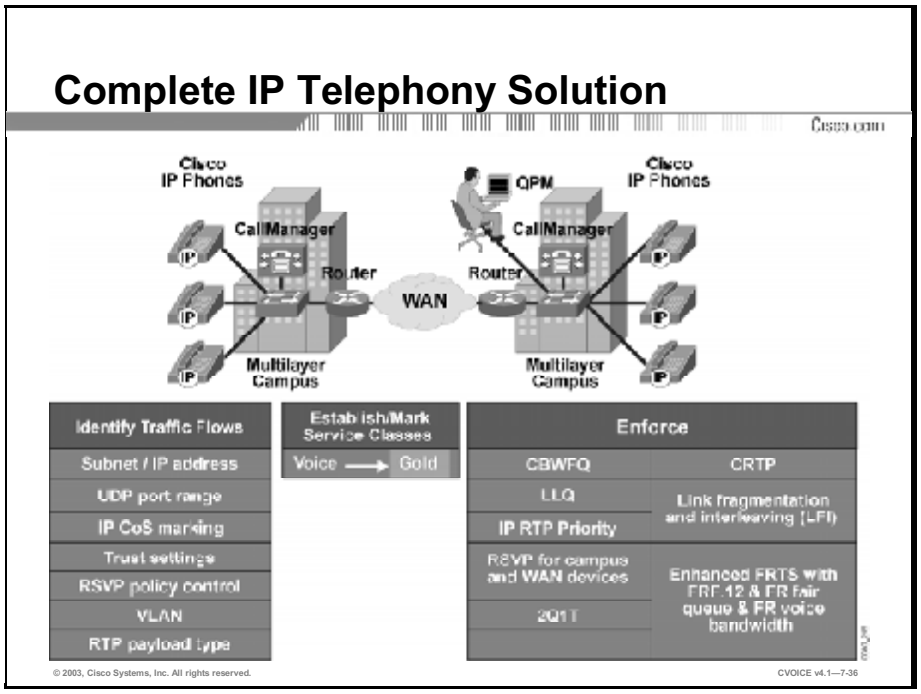
In networks today, users generally limit their application of intelligent tools in switches and routers for two reasons: fear of having inconsistent policies, or complexity and cost of implementing those policies in networks through Cisco IOS-based access control lists (ACLs). Therefore, the solution is to have a centralized policy control to manage network-wide QoS.



To effectively manage a voice and telephony-enabled network, administrators need tools that can simplify the configuration, deployment, management, and monitoring of QoS policies. Effective QoS management is an ongoing process. It entails the following tasks:

- Baseline monitoring of critical traffic flows to determine the policies that are needed
- Classifying applications into service classes
- Provisioning QoS with network-wide enforcement
- Validating QoS settings and results

The management tool must be able to deliver centralized QoS analysis and policy control for voice, video, and data networks. Additionally, the tool must enable network-wide, content-based DiffServ, and campus-to-WAN automated QoS configuration and deployment.

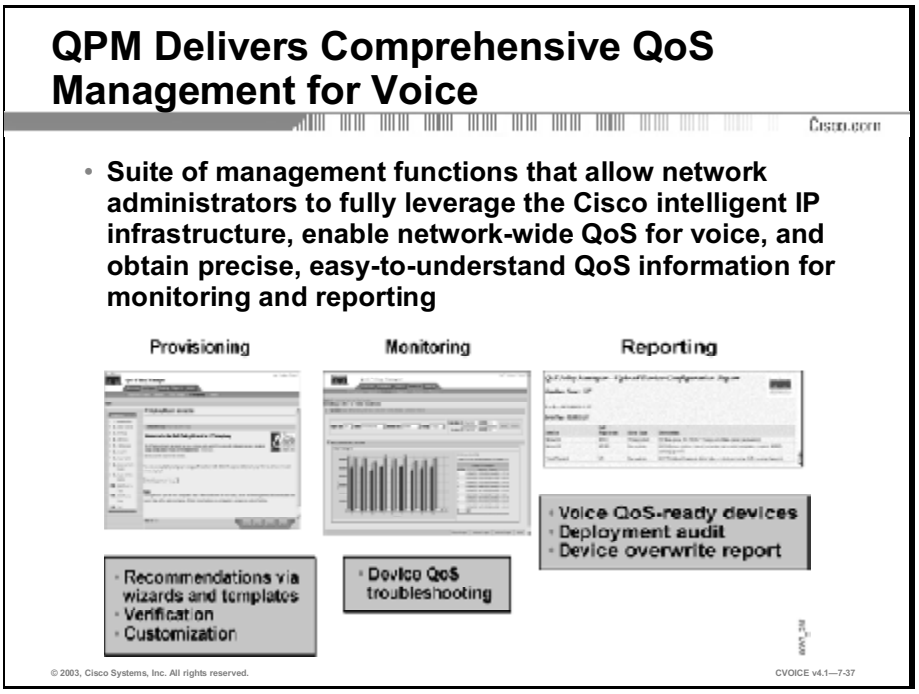


Using QPM, a network administrator quickly constructs rules-based QoS policies that identify and partition application traffic into multiple levels of service, ensuring that the most important applications receive priority service.

Example

A business may establish differentiated “Gold, Silver, and Bronze” levels of IP services. A Gold service guarantees latency and delivery for the transport of real-time traffic, such as VoIP. A Silver service guarantees delivery for business-critical applications that require certain response times but are not as latency-sensitive, such as enterprise resource planning (ERP) or e-commerce. A Bronze service can support certain web and e-mail sessions while other traffic is treated on a best-effort basis.

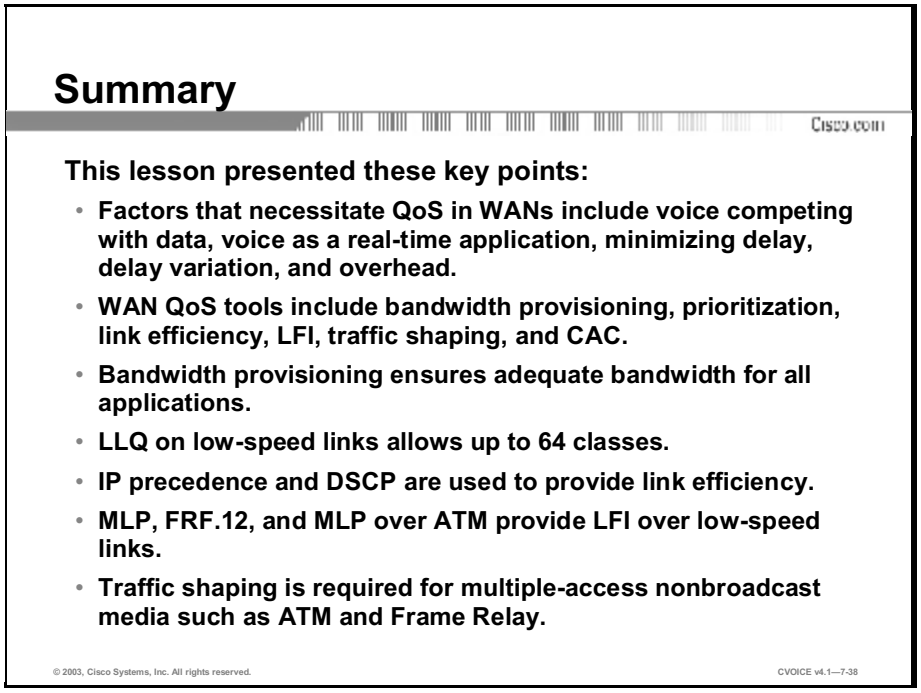
There are many QoS mechanisms built into Cisco Systems switches and routers to ensure that voice gets the required level of service in the network. QPM is an enabler for optimal voice quality in enterprise IP networks because it leverages the intelligent Cisco infrastructure to identify voice flows; for example, IP precedence, DSCP value, or RTP payload type. It also ensures that voice gets Gold service, and enforces low latency and low packet drops through various mechanisms; for example, placing LLQ on routers and voice packets in the priority queue (PQ) on Catalyst switches.

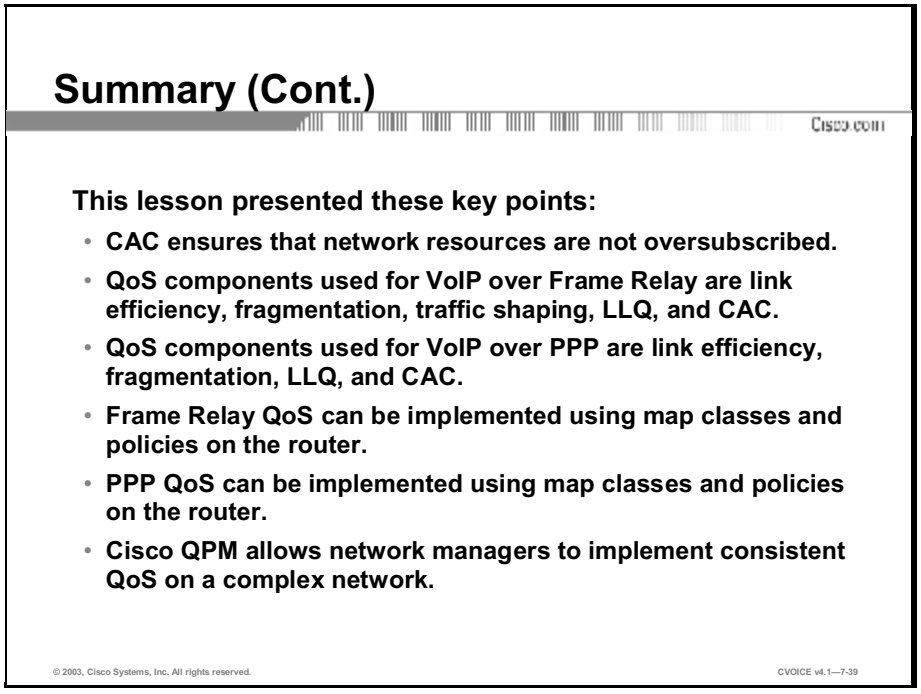


IP telephony usually requires a rather complex QoS configuration for the devices that carry voice traffic flows. IP telephony QoS management is one of the primary features of QPM. QPM includes a rules-based, step-by-step wizard with a built-in library of predefined QoS policy templates that are based on Cisco design recommendations. These policies allow for the accurate, speedy configuration of voice QoS mechanisms on switches and routers; they can also be modified as needed to meet specific network requirements. QPM includes a network voice-readiness report that lists devices that have all the required software and hardware to support QoS for voice. You can leverage QoS monitoring for troubleshooting and adjusting policies.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Applying Quality of Service in the WAN
- Assessment (Complex Lab): Refer to Lab 7-1, contained in Laboratory Exercises in Additional Resources section E.
- Call Admission Control lesson

References

For additional information, refer to these resources:

- "Voice over IP (VoIP) Frame Relay (VoFR) and ATM (VoATM)" http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Technologies&f=1533
- "Technical Support" http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking:Voice:QoS

Quiz: Applying Quality of Service in the WAN

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe six reasons for implementing QoS in a WAN
- List at least five QoS mechanisms that are used in a WAN
- Describe how bandwidth provisioning provides QoS in a WAN
- Illustrate how optimized queuing provides QoS in a WAN
- Describe how IP precedence and differentiated services code point provide link efficiency in a WAN
- List three link fragmentation and interleaving techniques that provide QoS in a WAN
- Identify the types of links that require traffic shaping
- Describe how Call Admission Control provides QoS in a WAN
- List five major components of QoS in a VoIP over Frame Relay network and describe three of those components
- List four major components of QoS in a VoIP over PPP network and describe one of those components
- Configure all QoS components on a VoIP over Frame Relay network using map classes and policies on the router
- Configure all QoS components on a VoIP over PPP network using map classes and policies on the router
- Describe the basics of QoS Policy Manager as a management tool for QoS

Instructions

Answer these questions:

Q1) Which characteristic describes voice traffic?

A) bursty

B) real-time

C) delay-tolerant

D) all of the above

Q2) Which requirement of voice adds significant overhead to the voice packets?

A) prioritization of voice packets

B) fragmenting the packets

C) numbering the packets

D) reducing the delay variation

Q3) Which two QoS mechanisms are commonly used on the WAN? (Choose two.)

A) bandwidth provisioning

B) queue scheduling

C) traffic shaping

D) separation of queues

E) marking of control and management traffic

Q4) Which OSI layer technology affects the type of QoS measures used in the WAN?

A) Layer 1

B) Layer 2

C) Layer 3

D) Layer 4

Q5) How much of the total available bandwidth should be consumed by minimum bandwidth requirements?

A) 100 percent of the bandwidth

B) no more than 99 percent of the bandwidth

C) no more than 80 percent of the bandwidth

D) no more than 75 percent of the bandwidth

Q6) Which two types of traffic are not included in the minimum bandwidth requirement calculation? (Choose two.)

A) voice media streams

B) video streams

C) HTTP traffic

D) H.323 traffic

E) overhead traffic

Q7) In optimized queuing, what kind of queuing do you use for voice control signaling protocols?

A) DSCP

B) FIFO

C) WFQ

D) CBWFQ

Q8) How many traffic classes does Low Latency Queuing allow for?

A) 32

B) 48

C) 56

D) 64

Q9) Describe two ways that DiffServ improves link efficiency in a WAN? (Choose two.)

A) by specifying how the device should forward the packet

B) by providing a finer granularity of priority setting for the applications

C) by providing a finer granularity of priority setting for the devices

D) by specifying the range of acceptable link speeds

Q10) What is the size of the CoS field that is used for IP precedence in an IP packet header?

A) 3 bits

B) 4 bits

C) 7 bits

D) 8 bits

Q11) When should you use QoS techniques that provide LFI?

A) when the speed of the link is less than 56 kbps

B) when the speed of the link is less than 768 kbps

C) when the speed of the link is greater than 786 kbps

D) when the speed of the link is less than 1544 kbps

Q12) Which technique is used for providing LFI on Frame Relay links?

A) MLP

B) MLP over ATM

C) FRF.12

D) G.711

E) G.729

Q13) Which type of links is traffic shaping NOT suitable for?

A) ATM links

B) Frame Relay links

C) Ethernet

D) links with variable access speeds

Q14) On what type of links can traffic-shaping mechanisms be used to limit jitter?

A) Frame Relay links

B) ATM links

C) point-to-point links

D) all of the above

Q15) Which statement describes CAC as a QoS technique?

A) specifies bandwidth for a link

B) frees up bandwidth for higher-priority traffic

C) reroutes calls that exceed the specified bandwidth

D) all of the above

Q16) Which Cisco application can you use to implement CAC on an entire network?

A) Cisco IOS

B) Cisco CallManager

C) CiscoWorks 2000

D) IVR

Q17) Describe two ways that FRF.12 identifies fragmented frames? (Choose two.)

A) by adding an extended header to the frame

B) by including a 1-byte flag in the header

C) by fragmenting the packets into fixed-size frames

D) by adding sequence numbers to the frames

E) by sending FRF.12 signaling to the destination

Q18) If FRTS is enabled on a link, what happens to voice frames when the network becomes congested?

A) Frames that exceed specified bandwidth are rerouted over another link, such as a PSTN.

B) Frames that exceed specified bandwidth are buffered and transmitted when congestion is reduced.

C) Frames that exceed specified bandwidth are marked DE and dropped.

D) Frames that exceed specified bandwidth are fragmented and given sequence numbers.

Q19) What is the size of a typical G.729 voice packet?

A) 20 bytes

B) 66 bytes

C) 214 bytes

D) 1500 bytes

Q20) How does LFI reduce delay and jitter for voice traffic in a WAN?

A) It queues high-priority voice traffic ahead of data traffic.

B) It fragments large voice packets and interleaves data packets among the fragments.

C) It fragments large data packets and interleaves voice packets among the fragments.

D) It reroutes voice traffic over faster connections.

Q21) What is the purpose of a policy map?

A) defines the voice-signaling and traffic class maps

B) defines how the link resources are assigned to the map classes

C) assigns a queue for voice-signaling traffic

D) defines how to classify traffic that does not fall into a defined class

Q22) Which QoS mechanism must be enabled for **map-class** to start?

A) LFI

B) LLQ

C) CAC

D) traffic shaping

Q23) What is the purpose of the **class class-default** command?

A) defines the voice-signaling and traffic class maps

B) defines how the link resources are assigned to the map classes

C) assigns a queue for voice-signaling traffic

D) defines how to classify traffic that does not fall into a defined class

Q24) During VoIP over PPP configuration, which command must you set properly to calculate the correct fragment size?

A) **bandwidth**

B) **fragment-delay**

C) **class voice-traffic**

D) **ip precedence**

Q25) What is the biggest advantage of using an automated policy tool such as CiscoWorks QPM?

A) It is less expensive than applying the policies manually.

B) It avoids inconsistencies in end-to-end policy application on a complex network.

C) It uses factory-recommended default settings for all devices.

D) It integrates well with all types of networks.

Q26) What type of information is supplied by the network-voice readiness report provided by QPM?

A) devices with software and hardware required to support QoS for voice

B) times of least congestion on the network

C) links that are best suited for transporting voice traffic

D) all of the above

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Call Admission Control

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 reasons for call admission control (CAC) and its configuration parameters.

Importance

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:

- State the reasons for CAC
- 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 Resource Reservation Protocol
- Explain how to configure Resource Reservation Protocol in a Frame Relay network
- Explain how to configure Resource Reservation Protocol with PPP
- Explain how to configure call control CAC
- Describe the three distinct groups of CAC mechanisms
- State the two types of call admission that Cisco CallManager allows

Learner Skills and Knowledge

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

- Knowledge of basics of VoIP
- Knowledge of TCP/IP networks

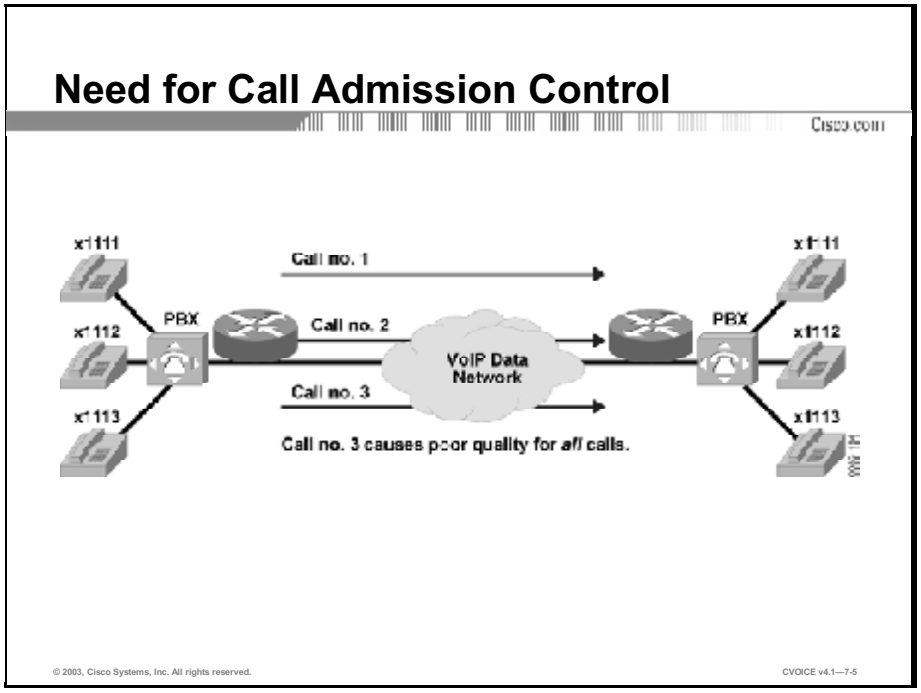
Outline

This lesson includes these sections:

- Overview
- Need for Call Admission Control
- Effects of Oversubscribing Bandwidth on Overall Voice Quality
- CAC as Part of Call Control Services
- Resource Reservation Protocol
- Configuration Examples: RSVP with Frame Relay
- Configuration Examples: RSVP with PPP
- Configuration Examples: Call Control CACs
- Other CAC Tools
- Cisco CallManager CAC
- Summary
- Assessment (Quiz): Call Admission Control
- Assessment (Complex Lab): Lab Exercise 7-2

Need for Call Admission Control

This topic explains why call admission control (CAC) is needed.



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

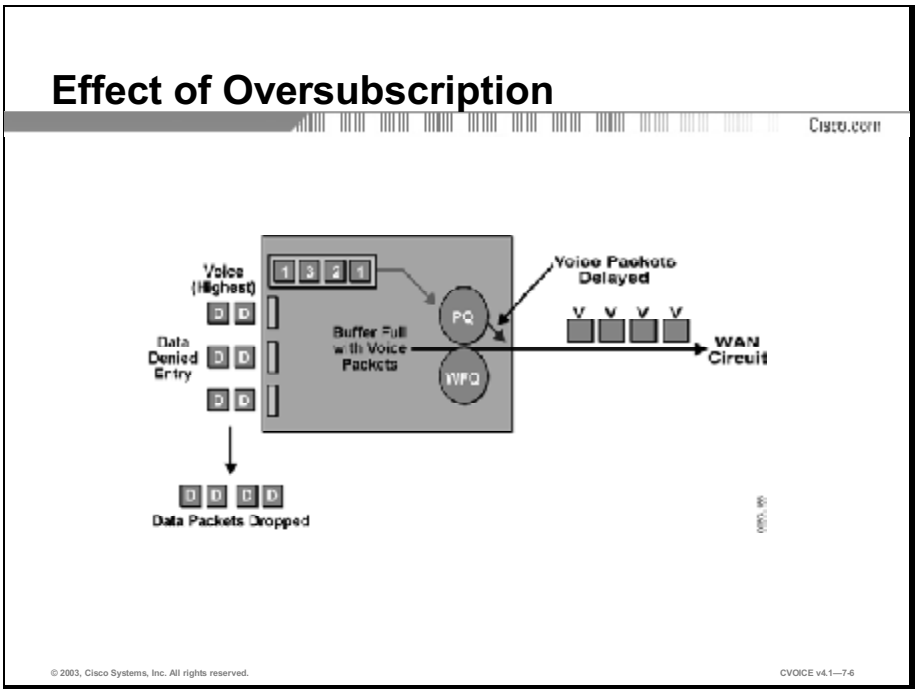
Because real-time traffic is sensitive to latency and packet loss, resolving network congestion when real-time traffic is present will jeopardize the quality of service (QoS). For real-time delay-sensitive traffic such as voice, it is better to deny network access under congestion conditions than to allow traffic on the network to be dropped and delayed. Dropped or delayed network traffic causes intermittent impaired QoS and results in customer dissatisfaction.

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

CAC mechanisms extend the capabilities of QoS tools to protect voice traffic from the negative effects of other voice traffic and to keep excess voice traffic off the network. The figure illustrates the need for CAC. If the WAN access link between the two PBXs has the bandwidth to carry only two Voice over IP (VoIP) calls, admitting the third call impairs the voice quality of all three calls.

Effects of Oversubscribing Bandwidth on Overall Voice Quality

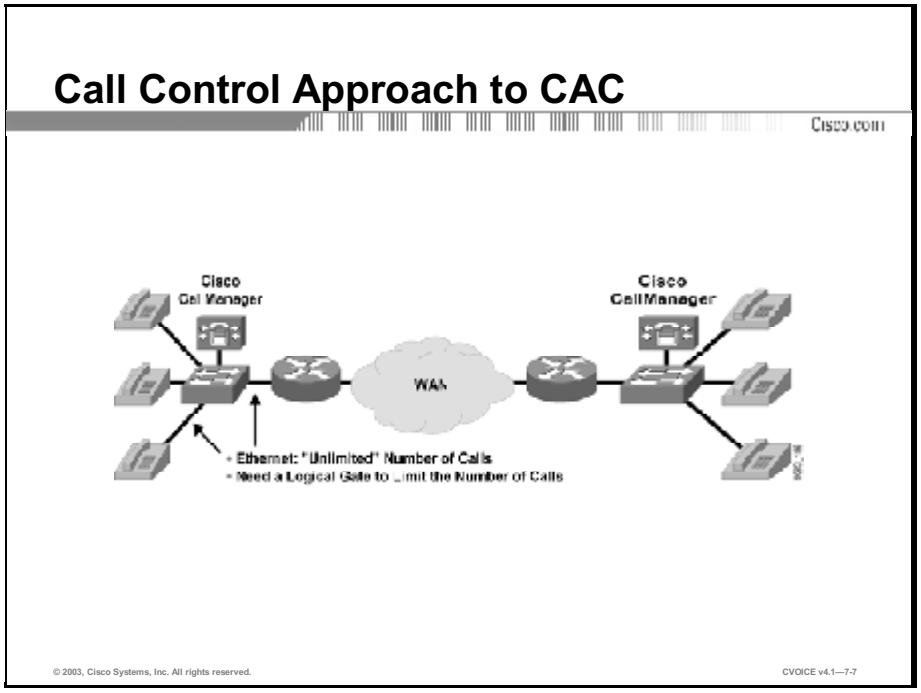
This topic describes the effects of network link oversubscription.



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 (LLQ).

CAC as Part of Call Control Services

This topic describes CAC as a function of call control services.



As you consider the many interesting aspects of CAC on packet networks, several solutions become evident. No one solution answers the entire problem, but the solutions all address a particular aspect of CAC.

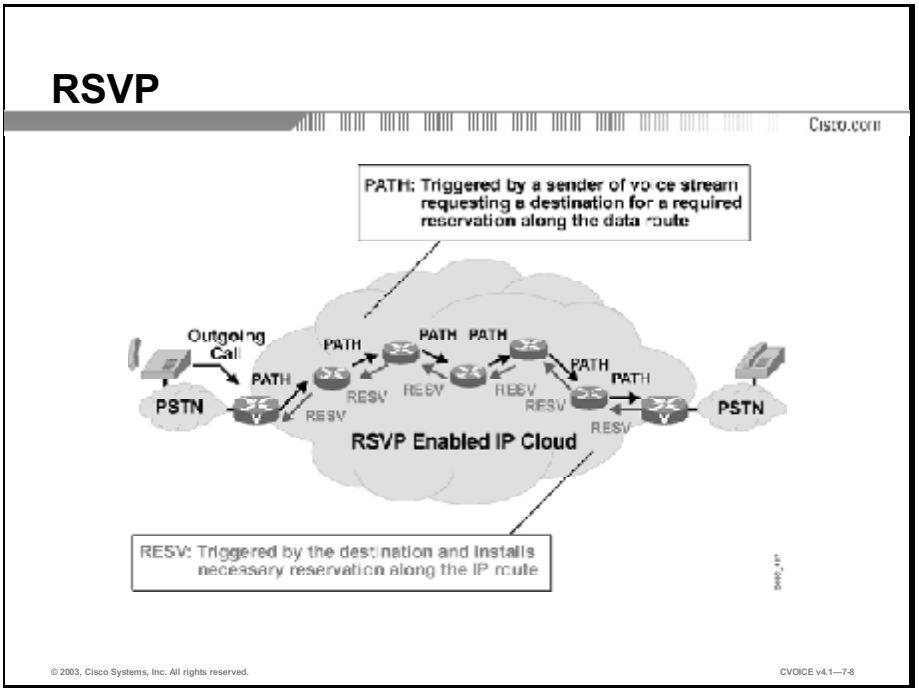
CAC, as part of call control services, functions on the outgoing gateway. CAC bases its decision on nodal information, such as the state of the outgoing LAN or WAN link. If the local packet network link is down, there is no point in executing complex decision logic based on the state of the rest of the network because that network is unreachable. Local mechanisms include configuration items that disallow all calls that exceed a specified number.

Example

If the network designer already knows that bandwidth limitations allow no more than five calls across the outgoing WAN link, then 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 Resource Reservation Protocol (RSVP).



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

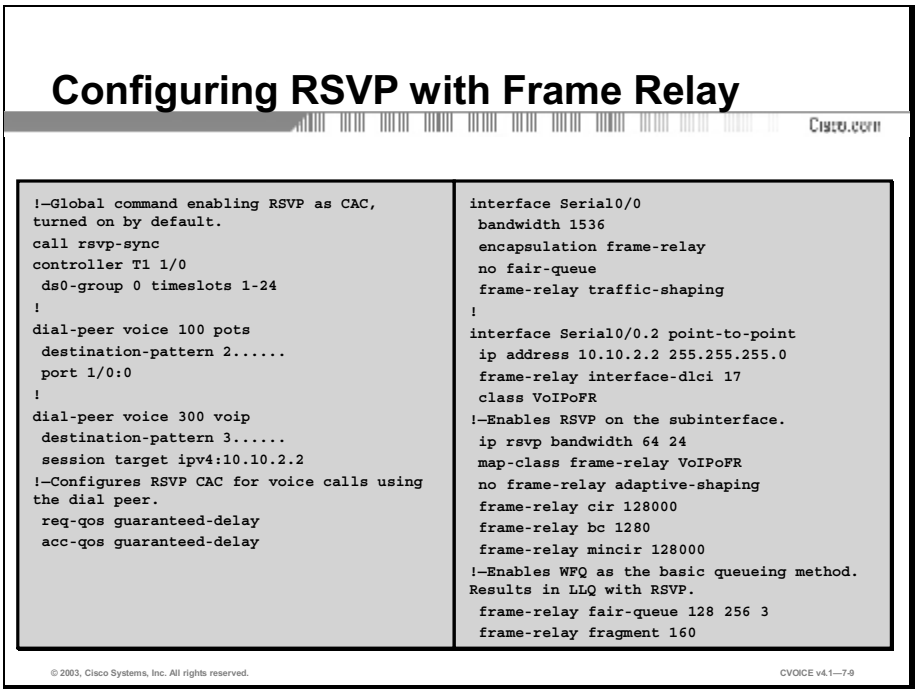
The terminating gateway ultimately makes the CAC decision based on whether both reservations succeed. At that point, the H.323 state machine continues with either an H.225 Alerting/Connect (the call is allowed and proceeds), or with an H.225 Reject/Release (the call is denied). The RSVP reservation is in place by the time the destination phone starts ringing and the caller hears ringback.

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

- The ability to maintain QoS for the duration of the call.
- An awareness of topology. In concept, the RSVP reservation installs on every interface that the call will traverse through the network. RSVP ensures bandwidth over every segment without any requirement to know 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. (It can have a scaling issue depending on how the network is designed.)
- RSVP provides 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.

Configuration Examples: RSVP with Frame Relay

This topic describes how to configure RSVP in a Frame Relay network.



You must perform the following three tasks on a gateway to originate or terminate voice traffic using RSVP with Frame Relay:

1. Turn on the synchronization feature between RSVP and H.323 using the **call rsvp-sync** command.

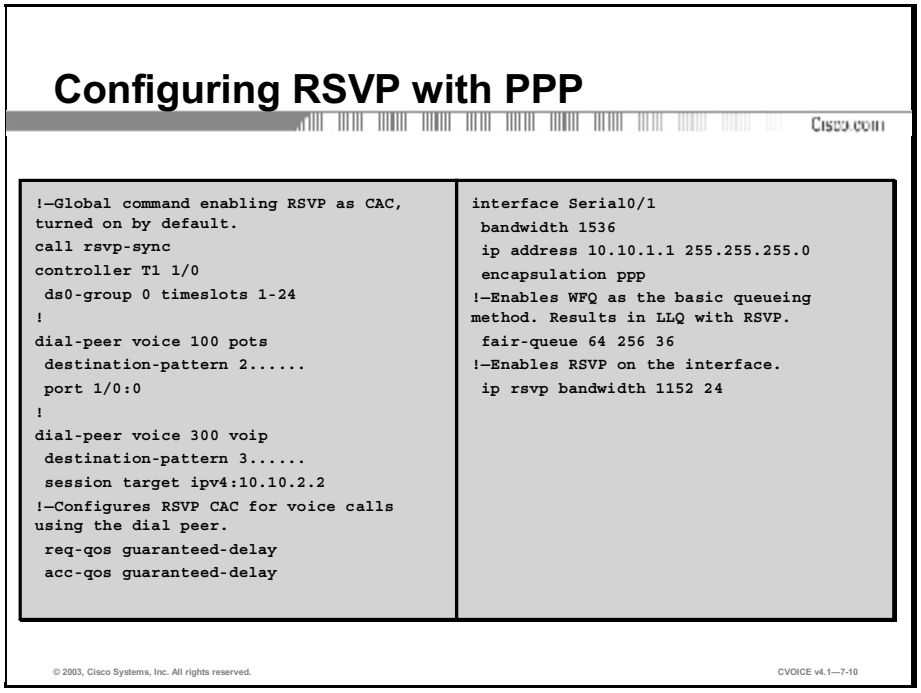
Note	This is a global command that is turned on by default when Cisco IOS® Release 12.1(5)T or later is loaded.

2. Configure RSVP on both the originating and terminating sides of the VoIP dial peers. Configure both the requested QoS (**req-qos**) and the acceptable QoS (**acc-qos**) using the **guaranteed-delay** command for RSVP to act as a CAC mechanism. Guaranteed delay ensures that the reservation is made only if the **req-qos** is met.

3. Enable RSVP and specify the maximum bandwidth on the Frame Relay interfaces that the call will traverse using the **ip rsvp bandwidth** command.

Configuration Examples: RSVP with PPP

This topic describes how to configure RSVP with PPP.



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

1. Turn on the synchronization feature between RSVP and H.323 using the **call rsvp-sync** command.

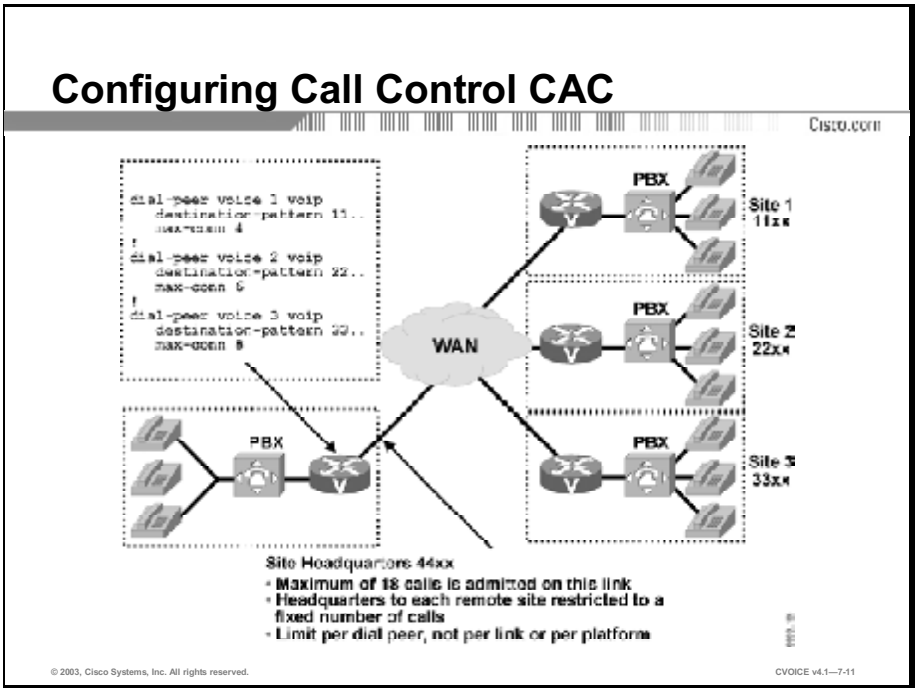
Note	This is a global command that is turned on by default when Cisco IOS Release 12.1(5)T or later is loaded.

2. Configure RSVP on both the originating and terminating sides of the VoIP dial peers. Configure both the requested QoS (**req-qos**) and the acceptable QoS (**acc-qos**) using the **guaranteed-delay** command for RSVP to act as a CAC mechanism. Guaranteed delay ensures that the reservation is made only if the **req-qos** is met.

3. Enable RSVP and specify the maximum bandwidth on the PPP interfaces that the call will traverse using the **ip rsvp bandwidth** command.

Configuration Examples: Call Control CAC

This topic describes how to configure call control CAC.



The max-connections CAC mechanism involves the use of the **max-conn** dial-peer configuration command on a dial peer of the outgoing gateway. This CAC mechanism restricts the number of concurrent connections that can be active on that dial peer at any one time.

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

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

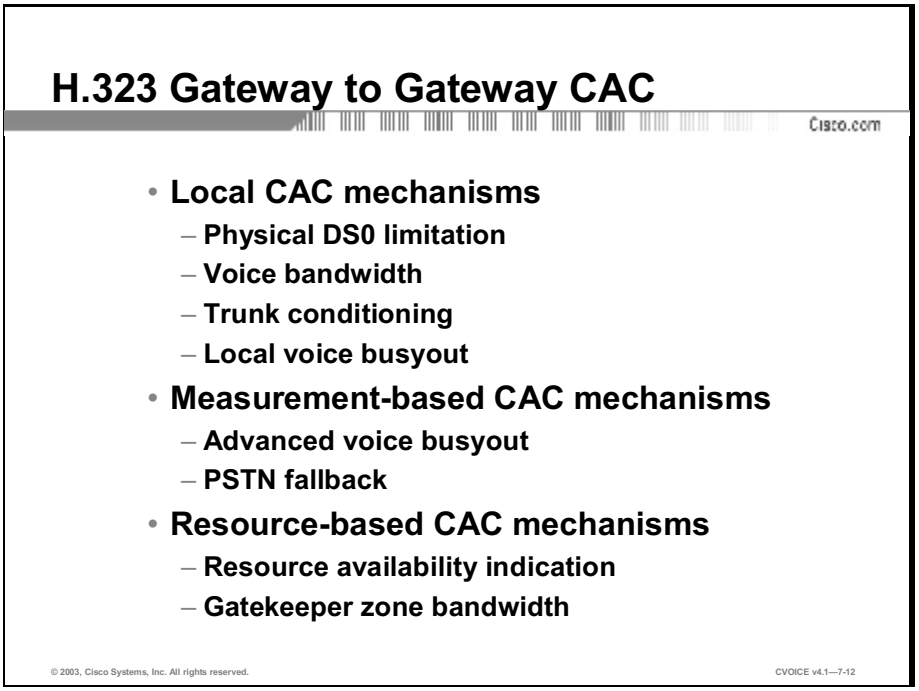
- For a relatively small number of dial peers that point calls to an egress WAN link, the sum of the individual **max-conn** dial-peer statements provides the maximum number of calls that can be simultaneously active across the WAN link.

- If the design objective is to limit the maximum number of calls between sites (rather than protecting the bandwidth of the egress WAN link), this can be a highly suitable feature. However, the dial peers must be structured in such a way that each remote site has one dial peer pointing calls each site.

The figure shows an example of this type of network. There are three remote sites, each with recognizable first digits in the dialing plan. The outgoing VoIP dial peers at the headquarters (HQ) site match the remote sites one-for-one. The number of calls to remote sites one, two, and three is limited to four, six, and eight respectively. Therefore, the egress WAN link can have no more than 18 active calls at any one time. In this configuration, the bandwidth of the link is provisioned for the most prudent number of calls.

Other CAC Tools

This topic enumerates other CAC tools and provides a link to learn more about them.



CAC mechanisms can be categorized into the following three distinct groups:

- **Local CAC mechanisms:** Local CAC mechanisms function on the outgoing gateway. The CAC decision is based on nodal information, such as the state of the outgoing LAN or WAN link. If the local packet network link is down, 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 more than a fixed number of calls. For example, if the network designer already knows that bandwidth limitations allow no more than five calls across the outgoing WAN link, then it seems logical that it should configure the local node to allow no more than five calls.

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

- **Resource-based CAC mechanisms:** Two types of resource-based mechanisms are those that calculate the resources that are needed and available and those reserving resources for the call. Resources of interest include link bandwidth, CPU power, memory, digital signal processors (DSPs), and digital service zero (DS0) time slots on the connecting time-division multiplexing (TDM) trunks. Several of these resources could be constrained at any one or more of the nodes that the call traverses on the way to its destination.

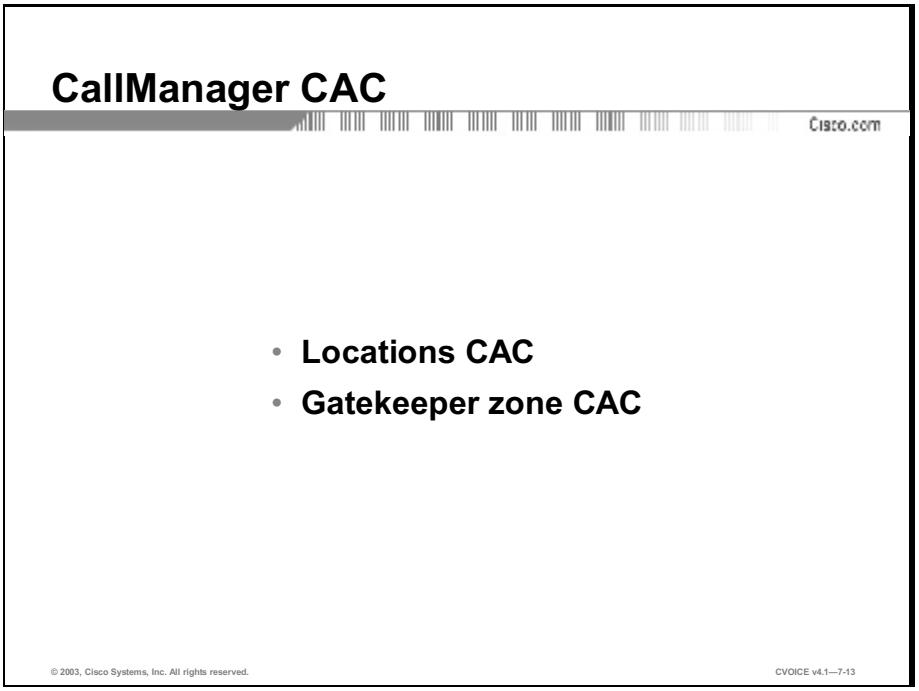
There is little overlap between local CAC mechanisms and those that look ahead to the rest of the network to determine nonlocal conditions. However, there is considerable overlap between the measurement techniques and the resource reservation techniques of the two "cloud look-ahead" CAC mechanisms. For this reason, there is debate over which is the better method.

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

Reference For more information on resource-based CAC mechanisms and other CAC tools, refer to the following topic on the Cisco.com website:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/cac.htm#77341

Cisco CallManager CAC

This topic describes the types of call admission that are possible with Cisco CallManager CAC.



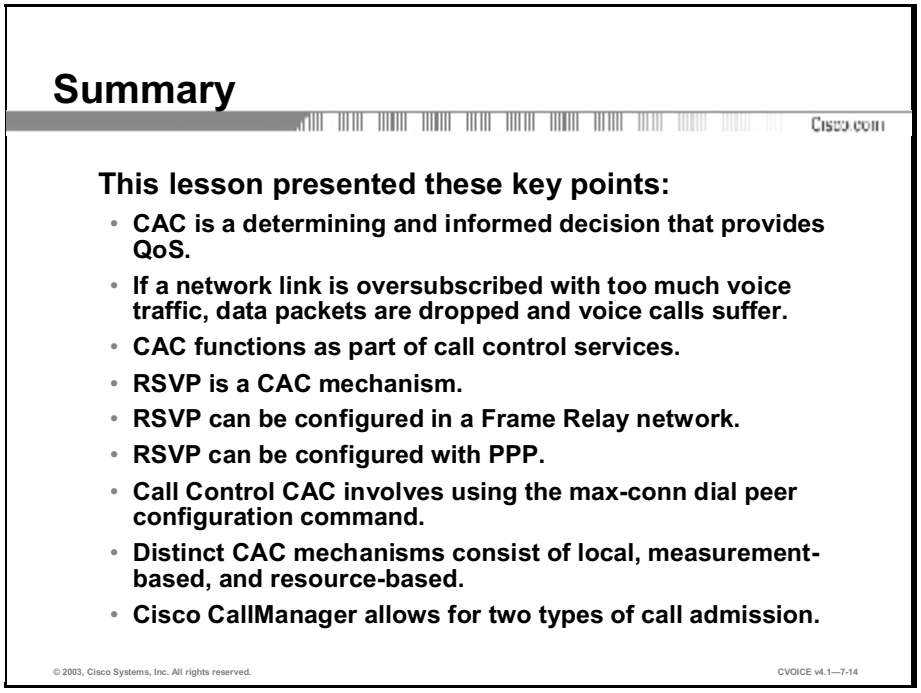
Using Cisco CallManager, the following two types of call admission are possible:

- **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.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Call Admission Control
- Assessment (Complex Lab): Refer to Lab 7-2, contained in Laboratory Exercises in Additional Resources section E.
- Voice Bandwidth Engineering lesson

References

For additional information, refer to these resources:

- "Resource-Based CAC Mechanisms" http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/cac.htm#77341

Quiz: Call Admission Control

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- State the reasons for CAC
- 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 Resource Reservation Protocol
- Explain how to configure Resource Reservation Protocol in a Frame Relay network
- Explain how to configure Resource Reservation Protocol with PPP
- Explain how to configure call control CAC
- Describe the three distinct groups of CAC mechanisms
- State the two types of call admission that Cisco CallManager allows

Instructions

Answer these questions:

Q1) What may happen to data packets when the network is congested?

A) The packets are dropped.

B) The packets are queued.

C) The packets are buffered.

D) All of the above.

Q2) What is the function of CAC?

A) to deny traffic that does not meet overhead requirements

B) to deny traffic that has not been authenticated

C) to deny voice traffic if the required network resources are not available

D) to deny data traffic until higher priority voice traffic has been transmitted

Q3) How is traffic affected if a link is oversubscribed?

A) Data packets are corrupted.

B) Data packets are dropped.

C) Voice quality suffers.

D) All of the above.

Q4) If CAC and queuing is 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

Q5) 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

Q6) 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.

Q7) 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 look-ahead”

C) guarantees QoS against changing network conditions

D) knows how many other calls are active on the link

Q8) 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

Q9) What is the function of the **guaranteed-delay** command?

A) configures the **req-qos** and the **acc-qos** on the link

B) ensures that the reservation is made only if the **req-qos** is met

C) enables buffering of voice packets

D) ensures that the reservation is made only if the acc-qos is met

Q10) Which command is turned on by default when Cisco IOS Release 12.1(5)T is loaded?

A) **ip rsvp bandwidth**

B) **guaranteed-delay**

C) **call rsvp-sync**

D) **req-qos**

E) **acc-qos**

Q11) Put the steps for configuring RSVP with PPP in the correct order.

_____ 1. Configure both **req-qos** and **acc-qos** using the **guaranteed-delay** command for RSVP to act as a CAC mechanism.

_____ 2. Turn on the synchronization feature between RSVP and H.323 using the **call rsvp-sync** command.

_____ 3. Use the **ip rsvp bandwidth** command to enable RSVP and specify the maximum bandwidth on the PPP interfaces that the call will traverse.

_____ 4. Configure RSVP on both the originating and terminating sides of the VoIP dial peers.

Q12) What is the **req-qos guaranteed-delay** command used for?

A) to specify required delay

B) to specify requested QoS

C) to request guaranteed delay

D) to request QoS services

Q13) The **max-conn** command is configured on _____.

A) the originating gateway

B) the terminating gateway

C) a dial peer of the outgoing gateway

D) a dial peer of the outgoing gatekeeper

Q14) Which situation is most suited to the use of the **max-conn** command to provide CAC?

A) when you want to limit the number of calls between sites

B) when you want to protect the bandwidth of the egress WAN link

C) when you want to protect the bandwidth of the ingress WAN link

D) when you have a large number of dial peers on the network

Q15) Which type of CAC mechanism involves sending probes to the destination IP address?

A) local CAC

B) measurement-based CAC

C) resource-based CAC

Q16) What type of information is typically compiled by measurement-based CAC techniques?

A) link bandwidth

B) loss characteristics

C) CPU power

D) available memory

E) delay characteristics

Q17) 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

Q18) Which device provides CAC for distributed call processing using Cisco CallManager?

A) DSP

B) dial peer

C) gatekeeper

D) gateway

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Voice Bandwidth Engineering

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 added voice.

Importance

Network administrators must be able to calculate existing bandwidth and added voice bandwidth to implement Voice over IP (VoIP).

Objectives

Upon completing this lesson, you will be able to:

- Describe the tools that are used to examine and collect traffic statistics
- Describe the network objectives for voice and data to ensure proper performance of the network
- Describe how to meet the network objectives within the current network
- Calculate the required number of trunks that are necessary to support voice traffic considering busy hour and dropped calls
- Calculate busy hour traffic
- Describe erlangs as they relate to trunks
- Explain three traffic probability assumptions when determining the number of trunks required to meet a Grade of Service

- Explain the purpose of traffic calculations
- Describe 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 fully benefit from this lesson, you must have these prerequisite skills and knowledge:

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

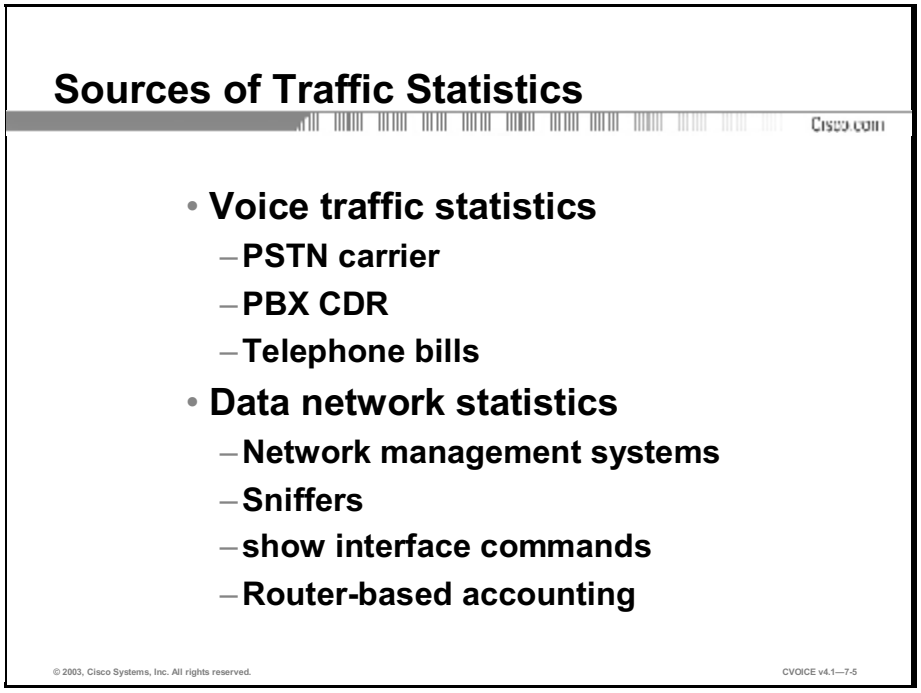
Outline

This lesson includes these sections:

- 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
- Assessment (Quiz): Voice Bandwidth Engineering

Sources of Traffic Statistics

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



Traffic engineering, as it applies to traditional voice networks, is 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 over X 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. You can gather voice traffic statistics from several sources including:

- public switched telephone network (PSTN) carriers
- Call detail records (CDR) in PBXs
- Telephone bills

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

- Peg counts 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.
- Grade of Service (GoS) rating for trunk groups.
- Total traffic 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 GoS.

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

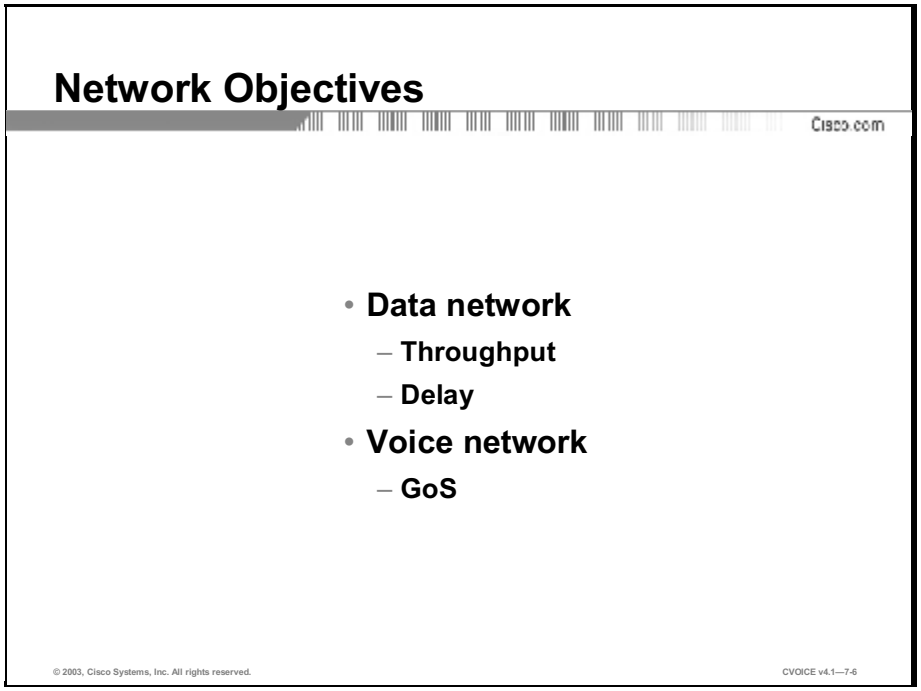
Unless the data network is accommodating voice and data on separate facilities, the resulting data traffic after migrating voice to the data network is the sum of the data traffic and the new voice traffic. Therefore, you must know how much bandwidth is required for data application.

You can gather data traffic statistics from:

- Network management systems (NMS)
- 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.



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.

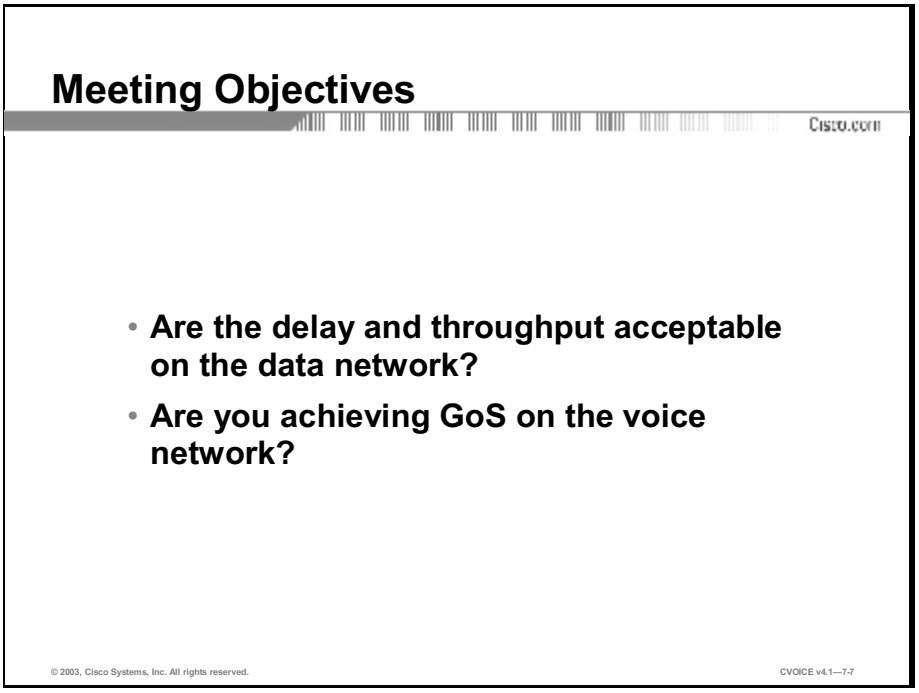
In a data network, users can reasonably expect to achieve a level of throughput in bits per second (bps) or a network transit delay in milliseconds (ms). Unfortunately, few networks have stated objectives for throughput and delay. In planning a combined voice and data network, voice is sharing the same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

Traffic engineering for voice is based on a target GoS. GoS is a unit that measures the chance that a call is blocked. For example, a GoS of P(.01) means that one call is blocked in 100 call attempts, and a GoS of P(.001) results in one blocked call per 1000 attempts. The GoS is usually defined for the peak or busiest period in the business day. In effect, the GoS represents service at its worst, during the busiest time of the day. During off-busy times, access to the service is better.

The GoS is an important parameter when calculating the number of trunks required to carry an amount of voice traffic.

Meeting the Current Network Objective

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



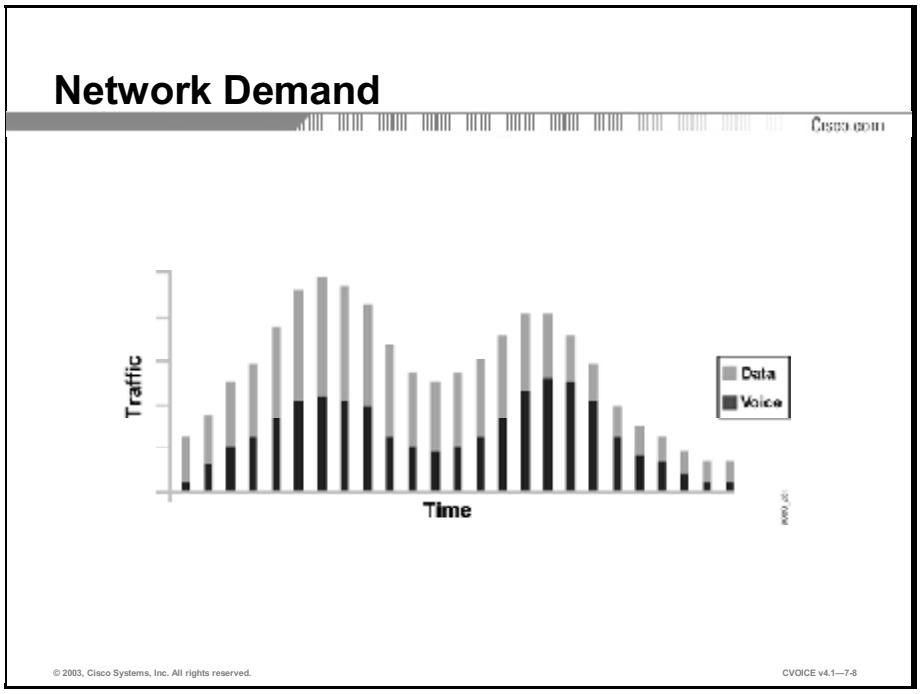
When the current level of voice and data traffic in the networks has been determined and objectives for throughput, delay (data traffic), and GoS (voice traffic) have been set, you should consider whether you are meeting the objectives in the current networks.

You might discover through your analysis of the voice and data networks that you are providing a poor GoS to your voice users, or 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, which is a mistake. Even worse, you could create an integrated voice and data network that behaves even more poorly.

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 GoS on the voice network?

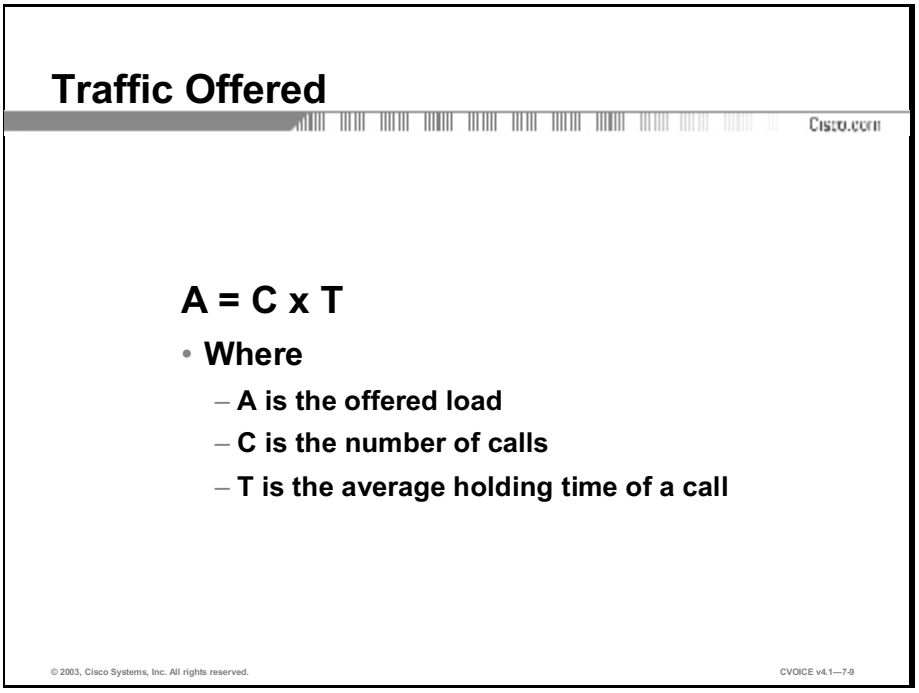
If you conclude that your network performance is below objectives, add a factor to your current traffic analysis for excessive demand.



You must understand how voice and data network demands relate to each other. If available, you should look at the relationship between the peak demands on each of the networks. This gives 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.

Traffic Theory

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



If you know the amount of traffic generated and the GoS required, then you can calculate the number of trunks required to meet your needs. Use the following simple equation to calculate traffic flow:

- A = C x 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, not *offered* traffic, as is usually provided by PBXs.

The holding time of a call (T) must account for the average time 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 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 calls x 0.5 minutes (overstated call length) = 202 excess call minutes
- Adjusted traffic (A): 1834 - 202 = 1632 actual call minutes

Another way to calculate this would be to use the formula A = C x 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 minutes (A) / calls (C)

T = 4.54 minutes

- **Corrected holding time (T):**

T = 4.54 – 0.50

T = 4.04 minutes

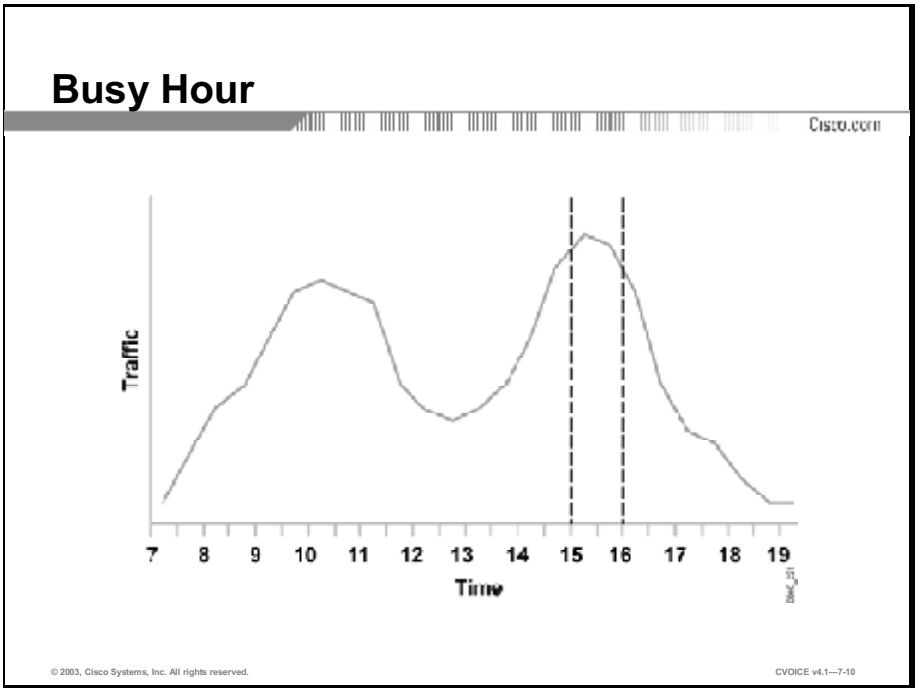
- **Adjusted traffic offered (A):**

A = 404 calls (C) x 4.04 minutes (T)

A = 1632 call minutes

Busy Hour

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

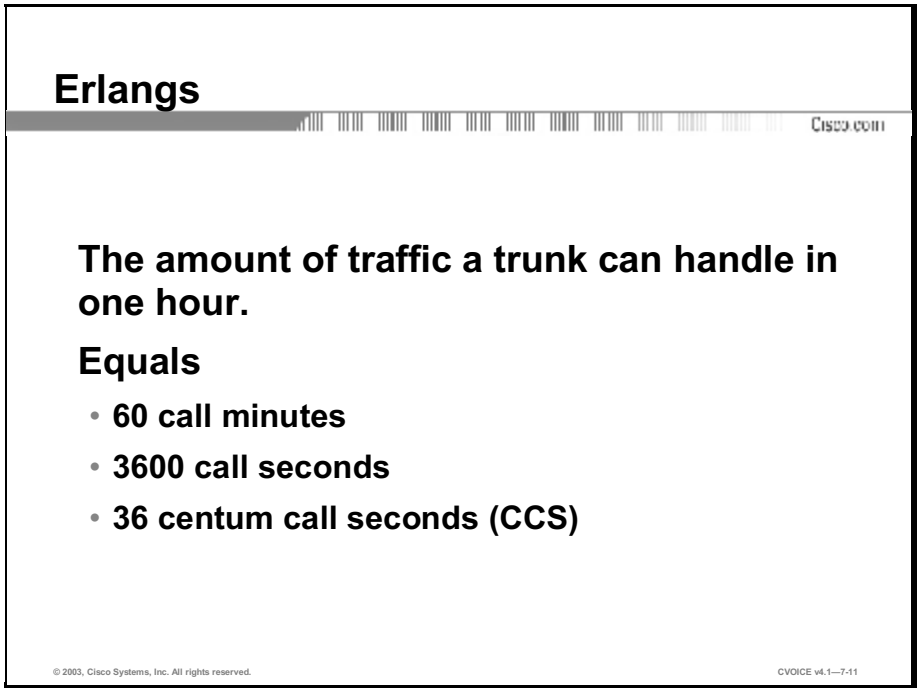


It is important to look at call attempts during the busiest hour of a day. The most accurate method of finding the busiest hour is to take the 10 busiest days in a year, sum the traffic on an hourly basis, find the busiest hour, and then derive the average amount of time.

In the absence of a traffic profile from which you can derive a precise value of the busy hour traffic, a simple way to calculate the busy hour is to collect one business month of traffic. 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 to 17 percent. As a rule, the busy-hour traffic represents 15 to 17 percent of the total traffic that occurs in one day. So, for example, if you have a trunk group that carries 66,000 minutes in one month or 3000 minutes per day on average (66,000/22), you could estimate the busy hour traffic by calculating 15 percent of the average daily traffic, or 3,000 x 15% = 450 minutes.

Erlangs

This topic describes erlangs.



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

Assume that 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 number of 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, or 1250 call minutes. However, erlangs is a measurement based on hours, so the number of erlangs is 1250 divided by 60, or 20.83 erlangs.

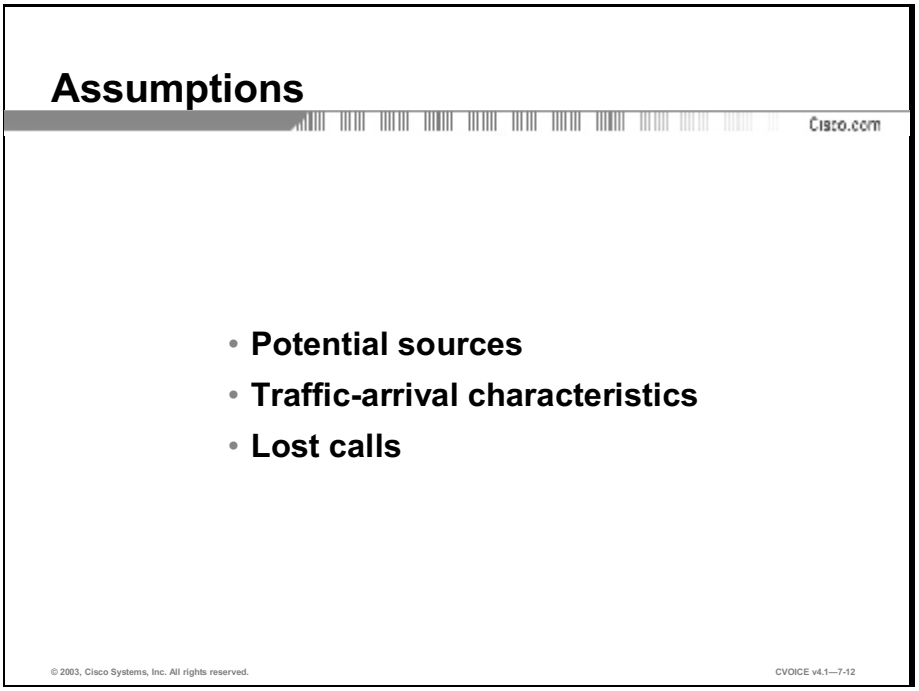
Note	The following calculation assumes that adjustments have been made to the average holding time.

Other equivalent measurements that you might encounter include:

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

Traffic Probability Assumptions

This topic explains three traffic probability assumptions to consider when determining the number of trunks required to meet a GoS.



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

- **Assumption 1:** 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.

- **Assumption 2:** Traffic arrival characteristics. Usually, this assumption is based on a *Poisson traffic distribution* (named after the mathematician who studied this extensively) where call arrivals follow a classic *bell-shaped* curve (hence bell curve). You commonly use Poisson distribution for infinite traffic sources. The arrival characteristics of traffic (calls) may be classified as random, smooth, or bursty.

Random arrivals are common with a large (tending to 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 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 provides the probability that you will receive 0 calls (very low probability), 100 calls (modest probability), 250 calls (the average, so the peak probability), 900 calls (very low probability), or any other number of calls.

Smooth traffic arrivals are common in applications where the traffic is dependent on other traffic, as in a telemarketing scenario. Smooth traffic arrivals are not modeled on the Poisson distribution due to their non-random nature.

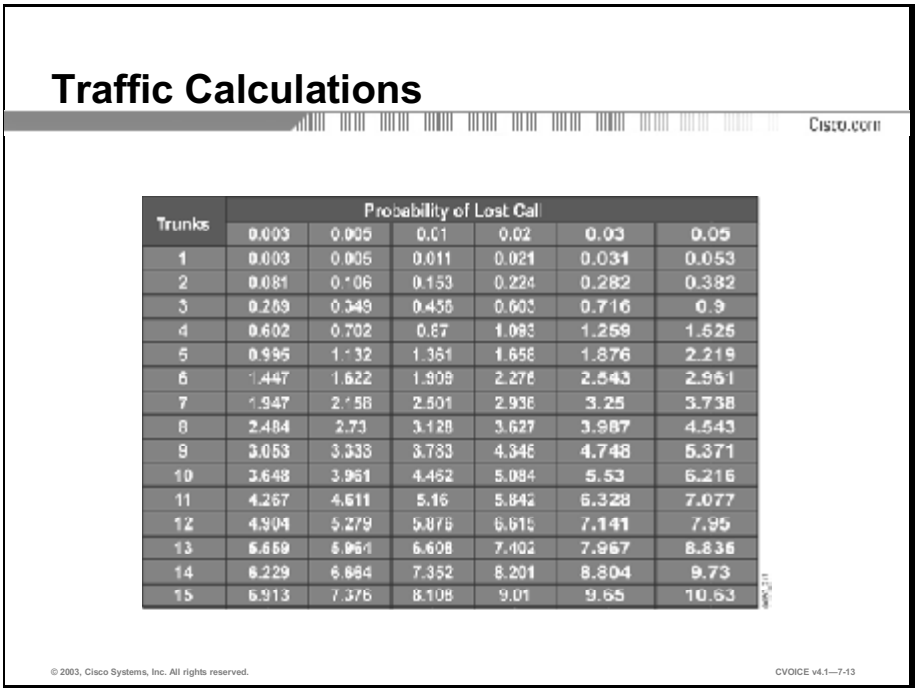
Bursty traffic arrivals are common in trunk overflow scenarios where excess overflow tends to occur for a short time and then disappear for an extended period of time. Bursty traffic is not modeled on the Poisson distribution because of its non-random nature.

- **Assumption 3:** 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 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. Recalling, or redialing, is an important traffic consideration. Suppose 200 calls are attempted. Forty 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 GoS 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 it uses the server for the full holding time. This assumption is most commonly used for automatic call distribution (ACD) systems.

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

Traffic Calculations

This topic explains the purpose of traffic calculations.



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 GoS, 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. As such, 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 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, but it is generally the most commonly used algorithm.

Example

A trunk group is a hunt group of parallel trunks. The following 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 the traffic occurs in the busy hour
- GoS p = .01
- Busy hour = 352 / 22 x 15% x 1.10 (call processing overhead) = 2.64 erlangs

The traffic assumptions are:

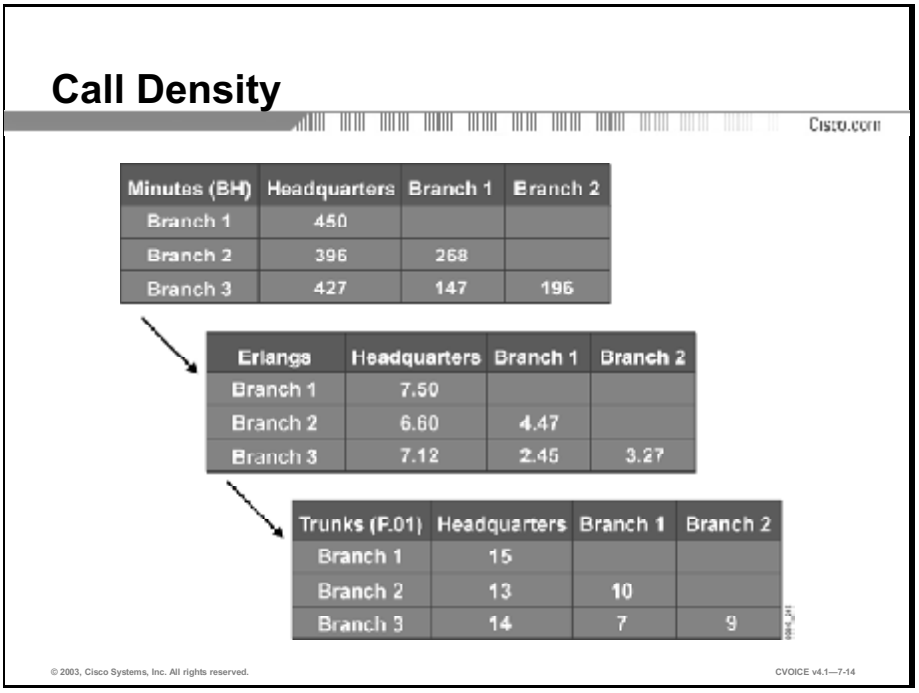
- Infinite sources
- Random or Poisson traffic distribution
- Lost calls are cleared

Based on these assumptions, the appropriate algorithm to use is Erlang B. You use the table in the preceding figure to determine the appropriate number of trunks (N) for a P of .01.

Because a GoS 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 a seven and eight trunk (*N*). 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.



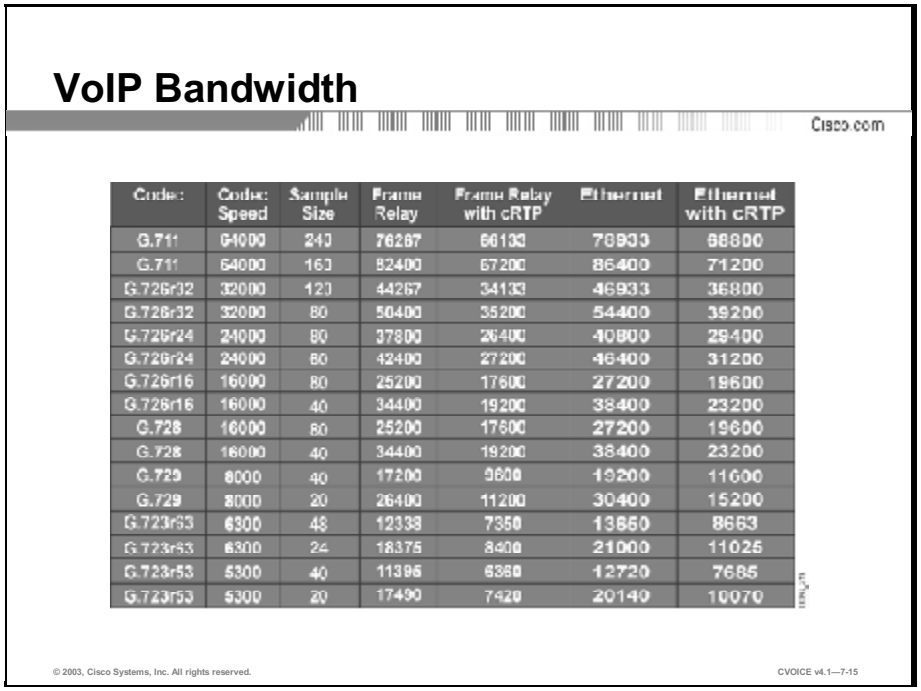
Unless your voice network is extremely small (two points, for example), calculating the trunk requirements between any two points in a network is a tedious task. One way to manage this more effectively is to design a *to/from* traffic matrix.

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.

The preceding figure shows this progression of sheets for a network with one headquarter and three branches.

Bandwidth Calculations

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



Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with cRTP	Ethernet	Ethernet with cRTP
G.711	64000	240	76267	66133	70933	66800
G.711	64000	160	82400	67200	86400	71200
G.726r32	32000	120	44267	34133	46933	36800
G.726r32	32000	80	50400	35200	54400	39200
G.726r24	24000	80	37800	26400	40800	29400
G.726r24	24000	60	42400	27200	46400	31200
G.726r16	16000	80	25200	17600	27200	19600
G.726r16	16000	40	34400	19200	38400	23200
G.728	16000	80	25200	17600	27200	19600
G.728	16000	40	34400	19200	38400	23200
G.729	8000	40	17200	9600	19200	11600
G.729	8000	20	26400	11200	30400	15200
G.723r63	6300	48	12338	7350	13650	8663
G.723r63	6300	24	18375	8400	21000	11025
G.723r53	5300	40	11396	6360	12720	7685
G.723r53	5300	20	17490	7420	20140	10070

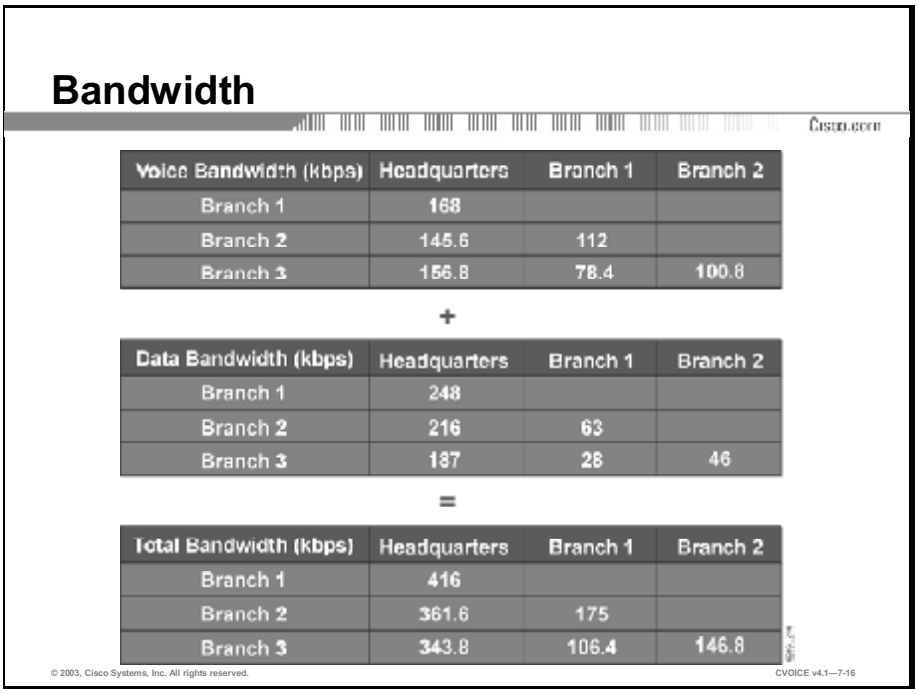
If you are provisioning a circuit-switched voice network, you must calculate how much traffic each of your trunks is expected to carry (according to theory), and investigate the most cost-effective way to provision each of the trunks.

Although you might still choose to perform the calculations used for Voice over IP (VoIP), for the purposes of this example, assume that all voice traffic is transported over the IP network. Consequently, you do not 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. When you estimate the VoIP bandwidth required for different coder-decoders (codecs) and over different datalinks, you can also calculate the benefit of compressed Real-Time Transport Protocol (RTP). These estimates of bandwidth for VoIP are shown in the figure.
2. When you identify the number of concurrent calls that you expect during the busy hour between points in the network, as a conservative (worst-case) first approximation to the bandwidth required for voice, you can simply multiply the number of concurrent calls by the bandwidth per call.



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

3. You may want to consider some refinements to this simple multiplier by considering the net benefits of bandwidth-reduction strategies, such as voice activity detection (VAD). VAD commonly reduces the bandwidth to between 60 and 70 percent of the original bandwidth. However, two animated talkers may not allow VAD to have any effect at all.
4. Finally, remember to add the budget for data applications to the bandwidth budget for voice.

Now that you have the total bandwidth budget, you must ensure that you do not overload the datalinks. Although it might seem most cost-effective to match the access rate on an interface to the total bandwidth budget, this is not correct.

On any network, dropped traffic and delays are proportional to the load on the 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

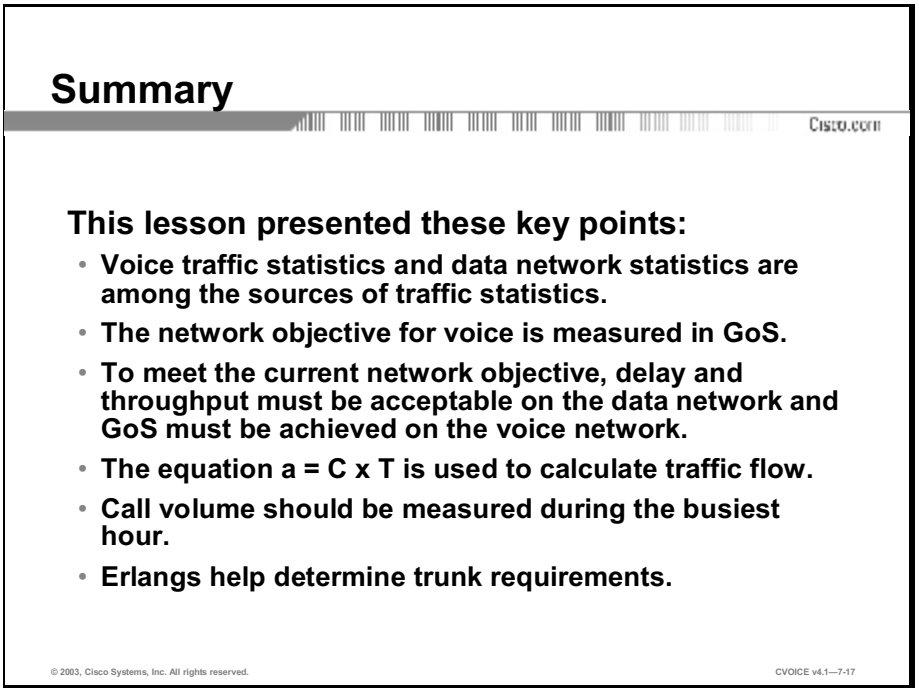
Capacity planning should take these factors into account, and link speed should be chosen to accommodate proper load factors. An ideal goal is to have demand equal to about 35 percent of total link speed.

To put these rules into the context of the example, the spreadsheet shows a demand for 416 kbps between Headquarters and Branch 1 during the busy (worst) 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, then the link speed must be 1,387 kbps or greater.

Based on the traffic in your network, you may be justified in aiming for a higher utilization of the links, but expecting full utilization is unrealistic. Setting too high a value results 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.

Summary

This topic summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Voice Bandwidth Engineering
- Scalable and Numbering Applications module

References

For additional information, refer to these resources:

- “Cisco Voice Design and Implementation Guide”
- “Cisco Traffic Analysis for Voice over IP”

Quiz: Voice Bandwidth Engineering

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the tools that are used to examine and collect traffic statistics
- Describe the network objectives for voice and data to ensure proper performance of the network
- Describe how to meet the network objectives within the current network
- Calculate the required number of trunks that are necessary to support voice traffic considering busy hour and dropped calls
- Calculate busy hour traffic
- Describe erlangs as they relate to trunks
- Explain three traffic probability assumptions when determining the number of trunks required to meet a GoS
- Explain the purpose of traffic calculations
- Describe 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

Instructions

Answer these questions:

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) GoS

D) packet loss

Q4) What type of statistics are measured by the GoS?

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 GoS

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 to 16 percent the length of the call

D) 10 to 16 times the length of the call

Q9) What will be the busy hour traffic if the traffic for one month is 15,400 minutes?

A) 77 minutes

B) 105 minutes

C) 116 minutes

D) 119 minutes

Q10) The most accurate method of finding the busiest hour is to take _____ in a year, sum the traffic on an hourly basis, find the busiest hour, and derive the average amount of time.

A) the total number of days

B) the 10 busiest days

C) 22 business days

D) 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 type of arrival traffic can be modeled on a Poisson distribution?

A) random arrivals

B) smooth arrivals

C) bursty arrivals

D) all of the above

Q14) Regarding treatment of lost calls, which possibility overstates the number of trunks required?

A) LCC

B) LCD

C) LCH

Q15) What is the most commonly used table for calculating the number of physical trunks required?

A) Poisson distribution

B) Erlang B

C) GoS 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) 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/from traffic matrix.

D) Use the A = C * T formula.

Q18) The call density matrix can be used to calculate the _____.

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

Q19) 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.

Q20) At what point can a voice and data network be said to have excessive load?

A) The averages demand over an 8-hour workday is 20 percent.

B) The average demand during the worst hour of the day is 30 percent.

C) The average demand over the worst 15 minutes of the day is 15 percent.

D) All of the above.

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

8

Scalable Numbering and Applications

Overview

This module describes attributes and implementation strategies for scalable numbering plans and applications of Voice over IP (VoIP) networks.

Upon completing this module, you will be able to:

- Access the need for and implement a scalable numbering plan in a VoIP network, given the growth patterns of a company
- Describe new and evolving applications and identify cost savings ideas that capitalize on the convergence of voice and data in an IP internetwork, given various business initiatives and customer requirements

Outline

The module contains these lessons:

- Building a Scalable Numbering Plan
- Applications

Building a Scalable Numbering Plan

Overview

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

Importance

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

Objectives

Upon completing this lesson, you will be able to:

- List four customer components that must be considered when implementing a scalable numbering plan and explain why this is important
- Describe the required attributes of a scalable numbering plan and list the benefits that adhering to them provides
- List the five attributes and advantages of a hierarchical numbering plan and describe the benefits they provide
- Describe the challenges associated with the integration of internal numbering with the public numbering plan
- Describe two methods that are used to integrate existing dial plans into a VoIP network

Learner Skills and Knowledge

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

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

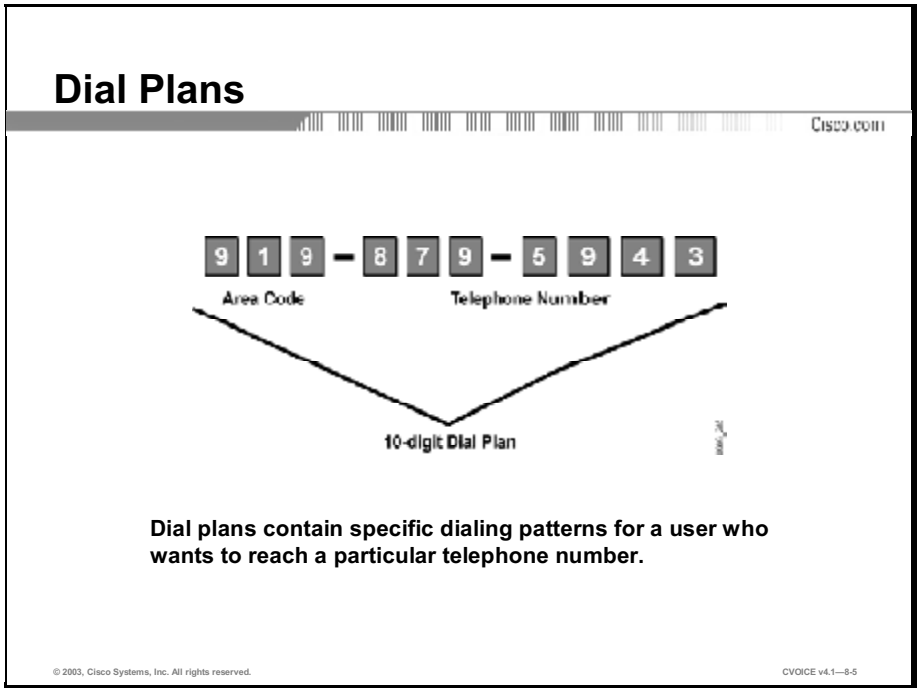
Outline

This lesson includes these sections:

- Overview
- Scalable Numbering Plan
- Scalable Numbering Plan Attributes
- Hierarchical Numbering Plans
- Internal Numbering and Public Numbering Plan Integration
- Enhancing and Extending an Existing Plan to Accommodate VoIP
- Summary
- Assessment (Quiz): Building a Scalable Numbering Plan

Scalable Numbering Plan

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



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

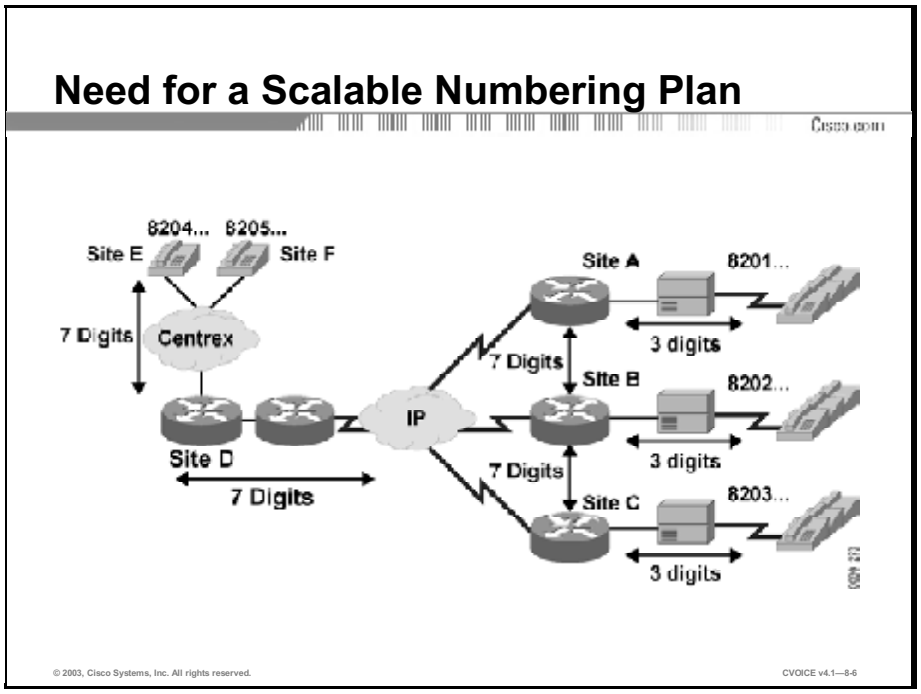
Example

The North American telephone network is designed around a 10-digit dial plan that consists of 3-digit area codes and 7-digit telephone numbers. For telephone numbers that are located within an area code, the Public Switched Telephone Network (PSTN) uses a 7-digit dial plan. Features within a central office (CO)-based PBX, such as Centrex, allow the use of a custom 5-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.

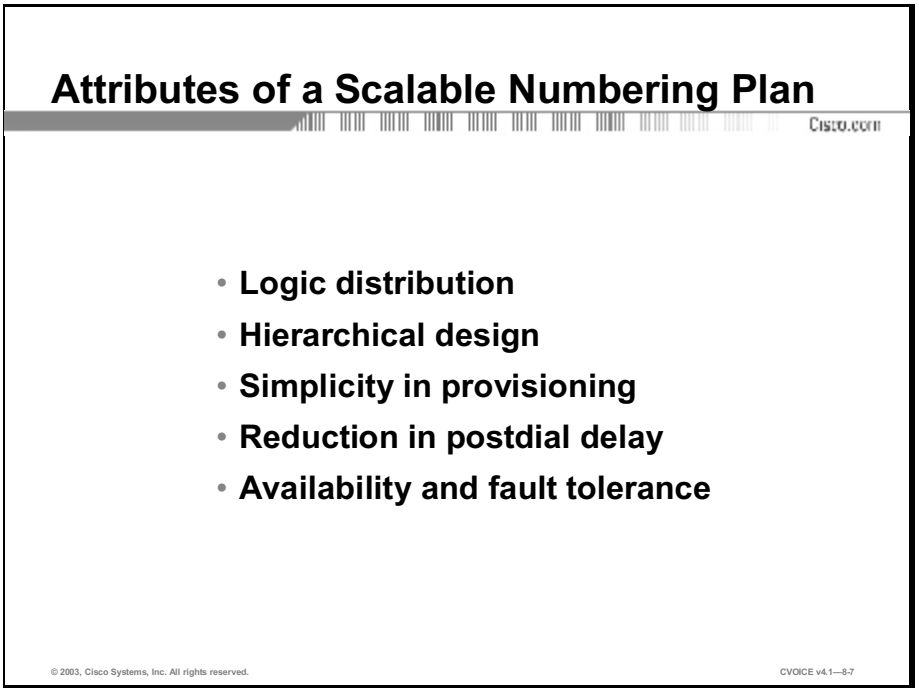
Typically, companies who implement VoIP networks carry voice traffic within the least expensive systems and paths. Implementing this type of system involves routing calls through IP networks, private trunks, PBXs, key systems, and the PSTN. The numbering plan to support the system is scalable, easily 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.



This figure illustrates a complex voice network that consists of the components discussed in this section. A comprehensive and scalable numbering plan must be well planned and implemented on networks such as this. The Centrex service requires 7-digit dialing between itself and Site D; the IP network requires 7-digit dialing toward Sites A, B, and C; and each of the PBXs require 3-digit dialing.

Scalable Numbering Plan Attributes

This topic describes the attributes of a scalable numbering plan.



When designing a large-scale numbering plan, you must adhere to the following 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.

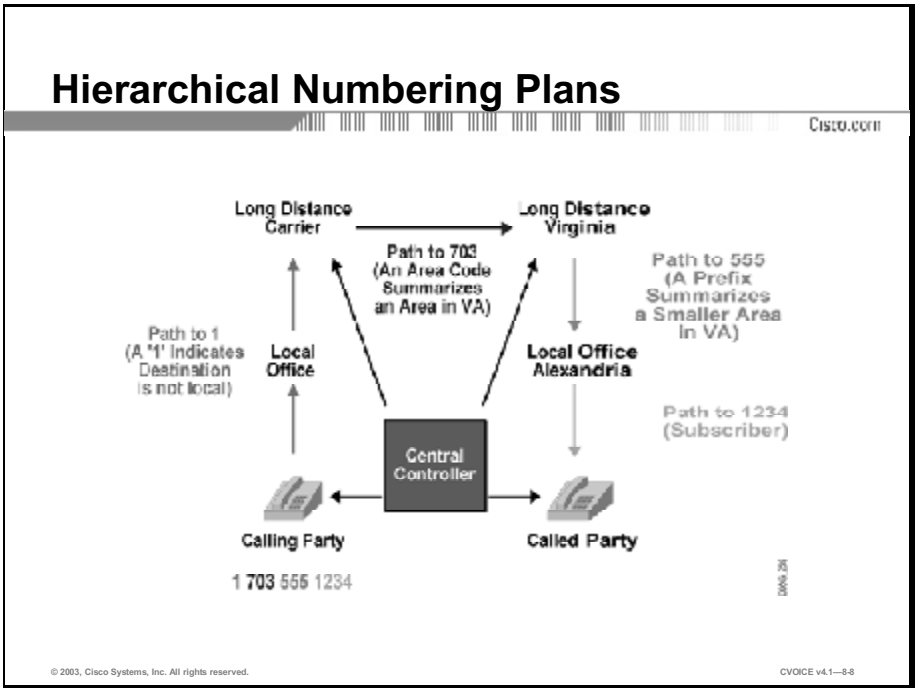
- **Simplicity in provisioning:** Keep the dial plan simple and symmetrical when designing a network. Try to keep consistent dial plans on the network by using translation rules to manipulate the local digit dialing patterns. These number patterns are normalized into a standard format or pattern before 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 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.

Hierarchical Numbering Plans

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



Scalable Internet routing protocols require telephone-numbering plans that are hierarchical. This design has the following advantages:

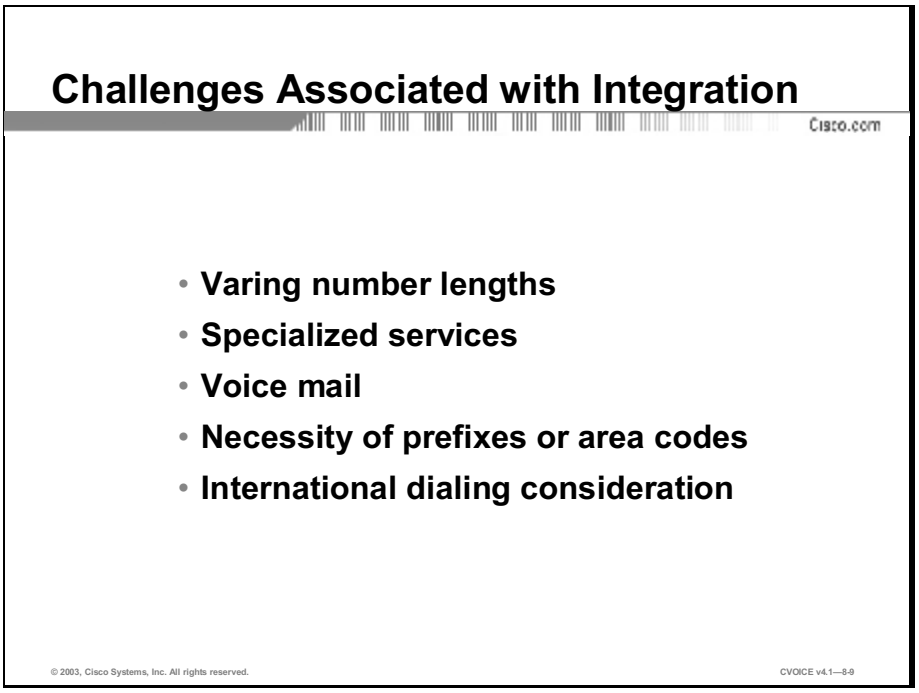
- **Simplified provisioning:** Provides the ability to add new groups and modify existing groups easily.
- **Simplified routing:** Keeps local calls local and uses a specialized number key, such as an area code, for long distance calls.
- **Summarization:** Establishes groups of numbers in a specific geographical area or functional group.
- **Scalability:** Adds scalability to the number plan by adding 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 (such as proprietary PBXs, key systems, and telephony services such as Centrex), and the necessity to conform to the PSTN at gateways, all 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 the following attributes.

- Minimal impact on existing systems
- Minimal impact on users of the system
- Minimal translation configuration
- Anticipated growth considered
- Conformance to public standards, where applicable

Internal Numbering and Public Numbering Plan Integration

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



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 International Telecommunications Union (ITU) developed the E.164 worldwide prefix scheme.

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

The challenges that you face with number plan integration are:

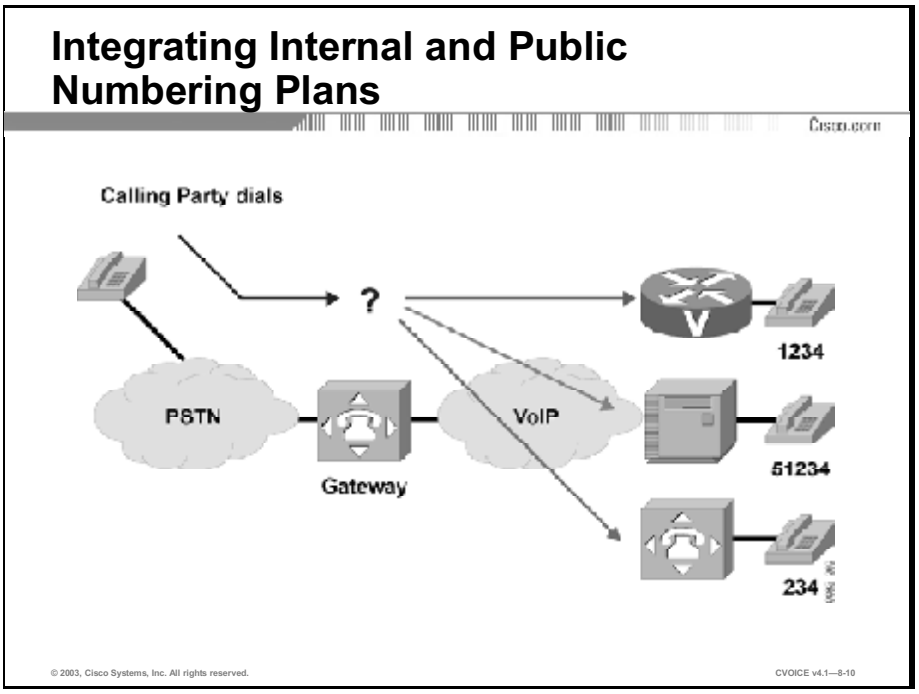
- **Varying number lengths:** Within the IP network, consideration is given to varying number lengths that exist outside the IP network. Local, long distance, key system, and Centrex dialing from within the IP network may require digit manipulation.

- **Specialized services:** Services such as Centrex and their equivalents typically have 4 or 5-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. Since the voice mail system can require a completely different number plan than the end-point 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 number plans vary in length within countries. Dialing through an IP network to another country requires careful consideration.

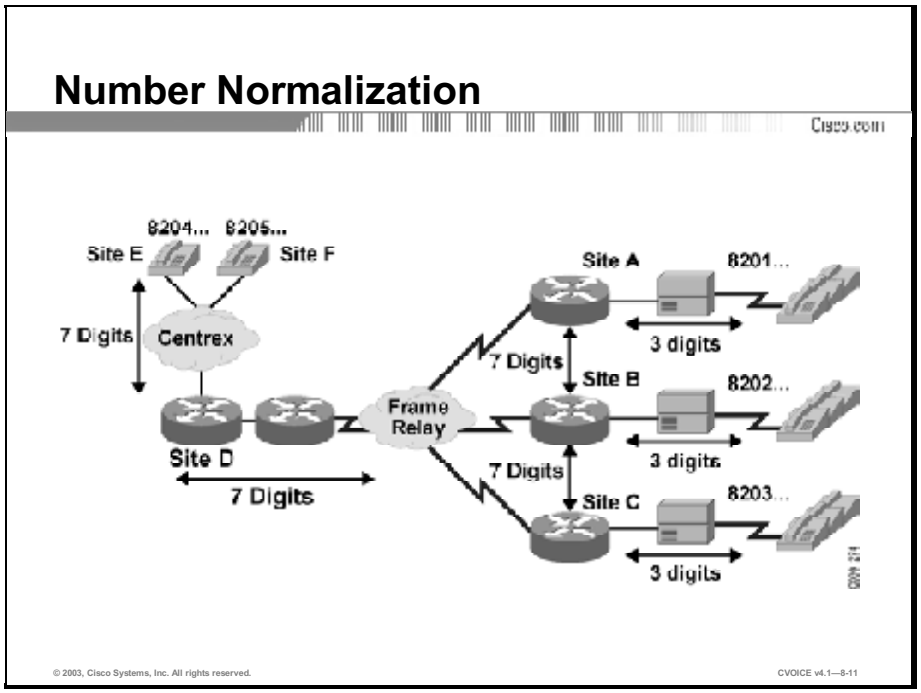


This figure shows a call from the PSTN destined for 1-703-555-1234. The gateway must realize the true destination. All endpoints end with the correct digit sequence, but which is the correct endpoint?

Should the gateway append or prepend digits to the dialed number? Should it strip and omit digits? Different PBXs support variable-length dial plans that contain 3 to 11 digits. The length variations present challenges when private plans merge with public number plans. Issues also arise when no one answers a number and the call is forwarded to a voice-mail system.

Enhancing and Extending an Existing Plan to Accommodate VoIP

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



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

Example

When site E (8204...) dials 8201999, the full 7-digit dialed string is passed through the Centrex to the router at site D. Router D matches the destination pattern 8201... and forwards the 7-digit dial string to router A. Router A matches the destination pattern 8201..., strips off the matching 8201, and forwards the remaining 3-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 7-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 4-digit prefix (in this case 8204), which results in forwarding the full dial string to the Centrex service.

Table 1: Router Digit Stripping Comparison

Router A	Router D
dial-peer voice 1 pots	dial-peer voice 4 pots
destination-pattern 8201...	destination-pattern 8204...
port 1/0:1	**no digit-strip**
!	port 1/0:1
dial-peer voice 4 vofr	!
destination-pattern 8204...	dial-peer voice 5 pots
session target s0 2	destination-pattern 8205...
!	**no digit-strip**
dial-peer voice 5 vofr	port 1/0:1
destination-pattern 8205...	!
session target s0 2	dial-peer voice 1 vofr
!	destination-pattern 8201...
	session target s0 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, class, or pool of gateways.

Example

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.

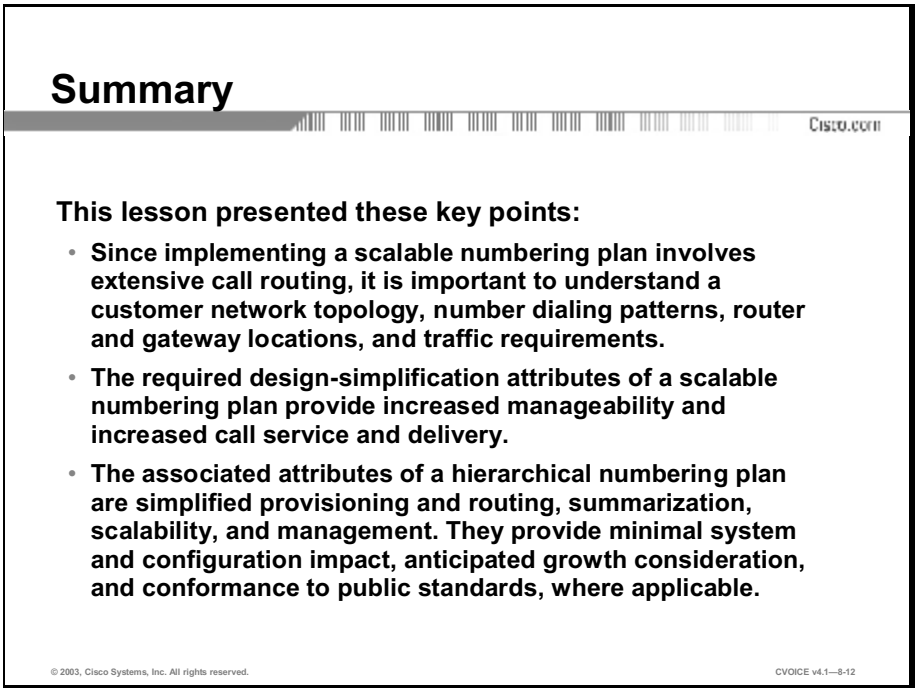
If the callers know the type of device that they are trying to reach, they can include the technology prefix in the destination address to indicate the type of gateway to use to get to the destination. For example, if a caller knows that address 2125551111 belongs to a regular telephone, the caller can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

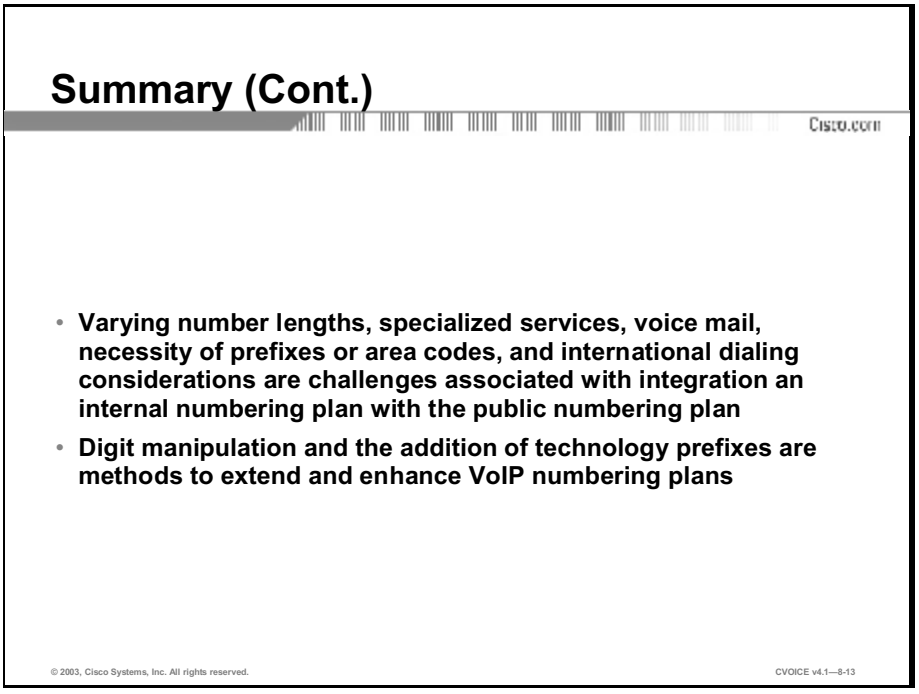
You can enter technology prefix commands on gateways and gatekeepers in two places, depending on how you want to design the technology prefix decision intelligence: the gateway VoIP interface or the gateway dial peer.

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.

Summary

This topic summarizes the key points discussed in this lesson.





Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Building a Scalable Numbering Plan
- Applications lesson

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
- "Voice-Understanding One Stage and Two Stage 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

Quiz: Building a Scalable Numbering Plan

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- List four customer components that must be considered when implementing a scalable numbering plan and explain why this is important
- Describe the required attributes of a scalable numbering plan and list the benefits adhering to them provides
- List the five attributes and advantages of a hierarchical numbering plan and describe the benefits they provide
- Describe the challenges associated with the integration of internal numbering with the public numbering plan
- Describe two methods that are used to integrate existing dial plans into a VoIP network

Instructions

Answer these questions:

Q1) The North American telephone-numbering plan is based on _____ digits.

A) 3

B) 7

C) 10

D) 11

Q2) What type of information do you need to design a dial plan for a customer?

A) network topology

B) traffic-routing requirements

C) current dialing patterns

D) proposed router and gateway locations

E) all of the above

Q3) 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

Q4) 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

Q5) 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

Q6) What 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

Q7) 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

Q8) Which worldwide prefix scheme was developed by ITU to standardize numbering plans?

A) G.114

B) E.164

C) G.164

D) E.114

Q9) Choose two locations where you can enter technology prefix commands. (Choose two.)

A) PBXs

B) gatekeepers

C) gateways

D) key systems

Q10) Technology prefixes can be used to identify _____.

A) type of gateway

B) class of gateway

C) pool of gateways

D) all of the above

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

Applications

Overview

This lesson describes various implementations and applications of Voice over IP (VoIP) networks.

Importance

Implementation of creative and cost-saving applications is the cornerstone of VoIP networks. Network administrators who have knowledge of various VoIP applications and successfully cut corporate costs bring added value to the bottom line.

Objectives

Upon completing this lesson, you will be able to:

- Describe the types of networks that implement Hoot and Holler networks and list two reasons businesses may choose this method of networking
- Explain how enterprise customers can avoid paying toll charges when making interoffice calls
- List the four components a hospitality enterprise can provide and explain the value it can bring to their business
- Explain how an IP Centrex can replace a PBX on a customer site and describe the services it provides
- List two candidates for multitenant applications and explain why building owners are beginning to build this type of network
- Describe the features and benefits of Cisco Voice Infrastructure and Applications, when using prepaid calling card services in a packet telephony network

- Describe the purpose of a computer telephony integration system and describe how it is accessed
- Describe how participants in a collaborative computing environment are connected and the benefit of this type of connection
- Explain how voice-enabled web applications work and why they are an alternative to the Internet
- Explain how call centers are changing to meet the needs of customers
- Describe how the Cisco brand of unified messaging system is used in an IP environment

Learner Skills and Knowledge

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

- Knowledge of VoIP networks
- Knowledge of telephony applications

Outline

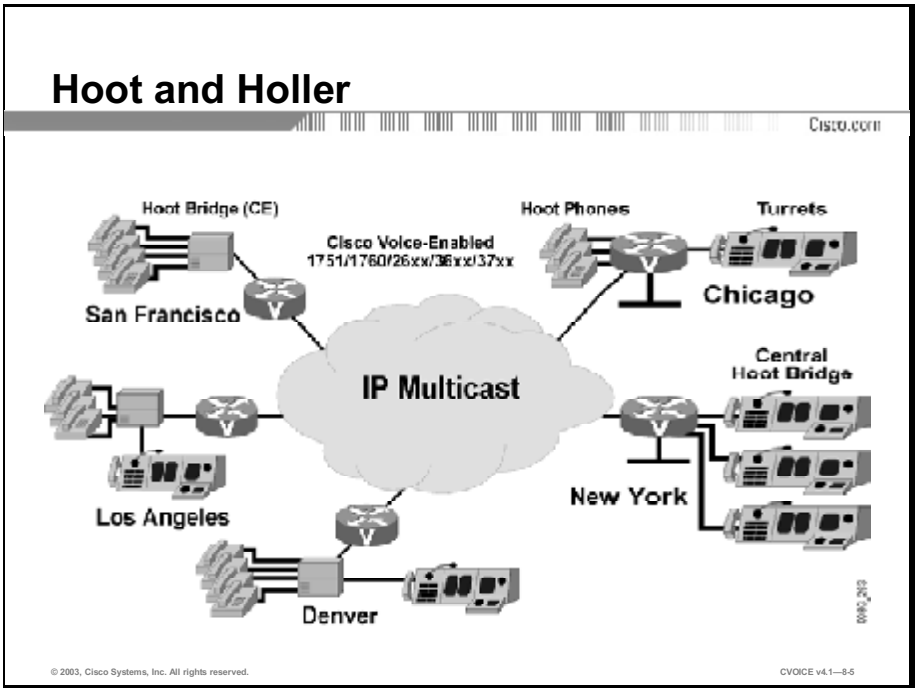
This lesson includes these topics:

- Overview
- Hoot and Holler
- Toll Bypass
- Hospitality
- IP Centrex
- Multitenant
- Prepaid Calling Card
- Computer Telephony Integration
- Collaborative Computing
- Voice-Enabled Web Applications

- Call Centers
- Unified Messaging
- Summary
- Assessment (Quiz): Applications

Hoot and Holler

This topic describes the Hoot and Holler implementations and applications.



A Hoot and Holler network (also known as a Junkyard Circuit, Squawk Box System, Holler Down Circuit, or Shout Down Circuit) provides “always on” multiuser conferences without requiring users to dial into a conference bridge. This type of network was devised more than 50 years ago when local concentrations of small, specialized businesses needed to communicate common, time-critical information. Junkyard operators up and down the East Coast of the United States were among the first users of these networks. They began to install their own telephone wires, speakers (called “squawk boxes”), and microphones to share information with other locations about parts that their customers needed. These networks functioned as crude, do-it-yourself, business-to-business intercom systems.

Hoot and Holler broadcast audio network systems have evolved into the specialized leased-line networks of today. Financial and brokerage firms use these networks to trade stocks and currency futures and provide time-critical information, such as market updates and morning reports. Users of various forms of Hoot and Holler networks include brokerages, news agencies, publishers, government and municipal emergency response agencies, weather bureaus, transportation providers, utility operators, manufacturers, collectibles dealers, talent agencies, airlines, and nationwide salvage yard organizations.

Hoot and Holler over IP transports Hoot and Holler voice traffic over traditional data networking equipment on an existing enterprise multiservice network. Hoot and Holler is another packet-based application that runs on a corporate multiservice network. Hoot and Holler enables businesses to eliminate expensive, dedicated leased lines, while protecting investments in existing Hoot and Holler equipment; for example, turrets, bridges, and four-wire telephones. In addition to eliminating the leased lines, running Hoot and Holler traffic over an

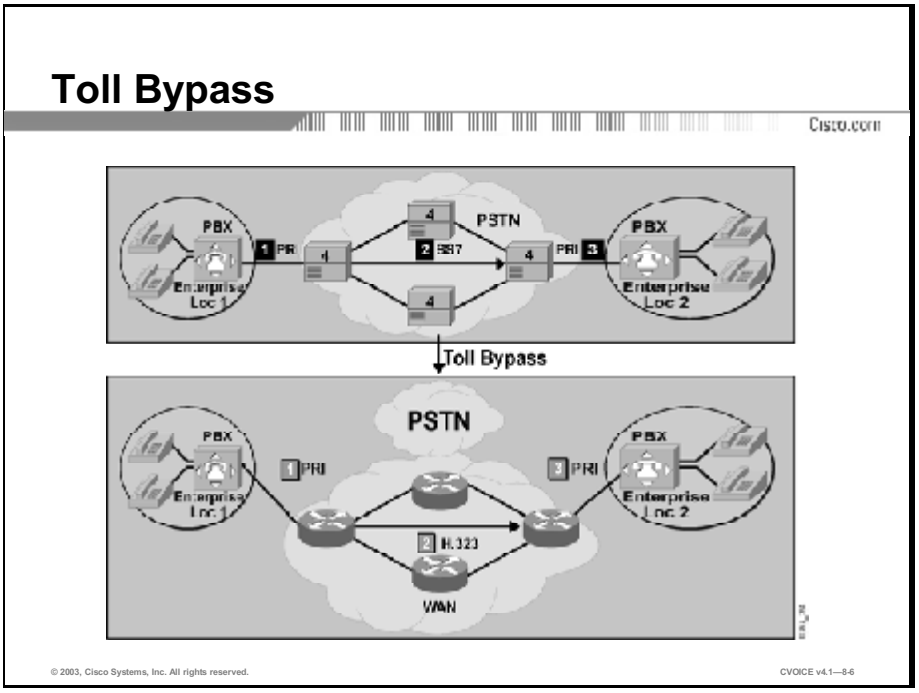
IP network allows businesses to utilize bandwidth more efficiently. When bandwidth is not being used for Hoot and Holler traffic, it can be made available for data.

Hoot and Holler requires that IP multicast is active on the routers that support the Hoot and Holler circuit. The connections are configured using special dial peers configured with “session protocol multicast.”

Reference For more information on multicast services, access the Cisco.com website at: http://www.cisco.com/ipmulticast

Toll Bypass

This topic describes the toll bypass implementations and applications.



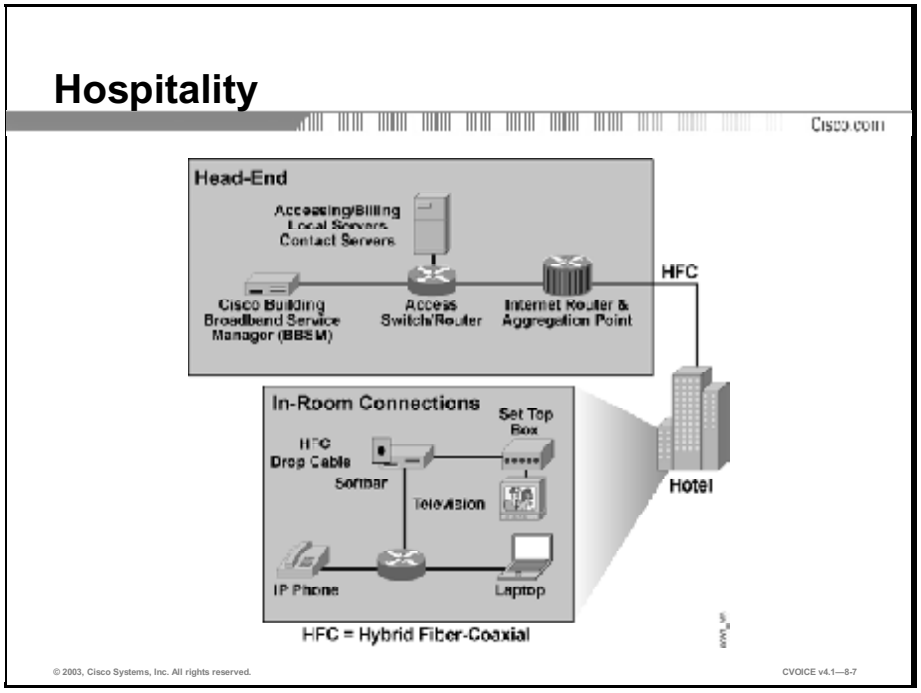
Toll bypass allows customers to bypass the Public Switched Telephone Network (PSTN). The PSTN consists of the tandem time-division multiplexing (TDM)-based switches to use the packet network for long-distance (or toll) voice calls. Enterprise customers who typically depend on the PSTN for their interoffice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

Example

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

Hospitality

This topic describes the hospitality implementations and applications.



Hospitality enterprises (for example, hotels, airports, and convention centers), host guests who demand high-speed connections to the Internet and access to telephony services. Enterprises with a large number of traveling users spend money to support LAN-like performance and extend high-speed telecommuting to corporate users.

Hospitality providers build networks that offer such services in a flexible, affordable, and transparent manner. Applications include fast Internet access and high-volume VoIP solutions. In hotels, one building or the entire hotel campus is wired with a single broadband access line to supply voice, video, and Internet applications to guest rooms. The hotel can take advantage of high-volume, long-distance discounts from their provider while realizing revenue from direct long-distance dialing by hotel guests. A hospitality environment can deploy the following components:

- **Cisco Building Broadband Service Manager (BBSM):** This service-creation platform enables hotel property owners to create, market, and operate broadband access services. BBSM provides plug-and-play access, customizable portals to restaurants, wineries, and retail shops, and support for multiple authentication and billing options.

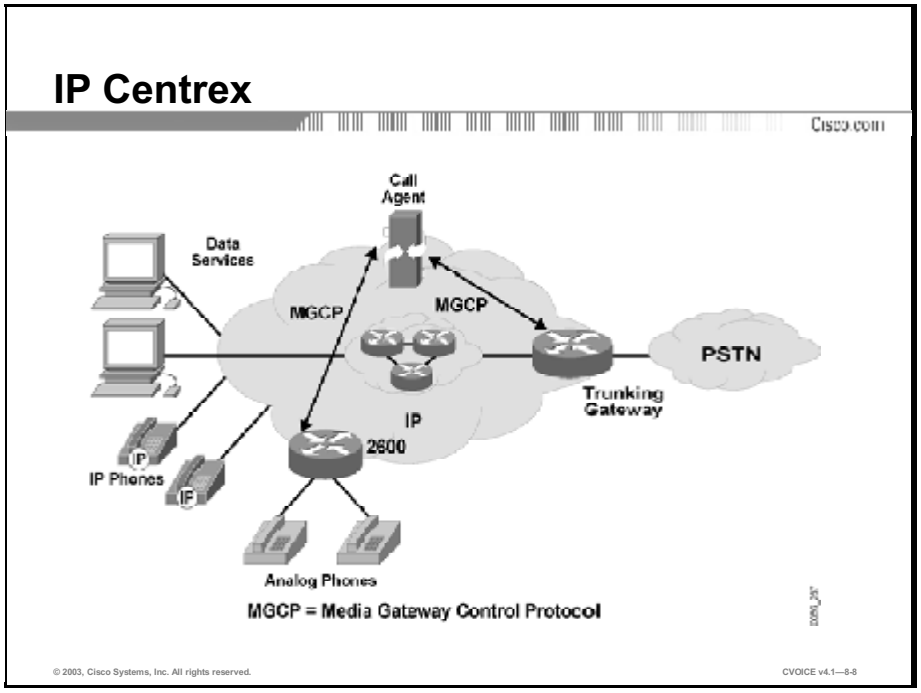
- **Cisco Integrated Communications System (ICS):** This integrated platform combines the essential elements of an IP telephony system, such as call-processing and voice applications, voice-trunking, and data routing, into a single platform that is easy to deploy and manage. The modular design of the Cisco ICS provides a hotel, for example, with the flexibility to choose the converged applications that guests require and add new functionality and applications when necessary.

- **Cisco IP Phone:** This system provides hotel guests with added conveniences, such as telephone-based concierge services, linked directories to local attractions, and automatic speed dial setup. For groups taking advantage of meeting services, the Cisco IP Phones provide personalized group directories, meeting agenda and room locations, and broadcast alert capabilities.

- **Cisco Content Transformation Engine (CTE):** The CTE is an appliance-based solution that optimizes the delivery of web content to a variety of wireless and wired devices, such as cell phones, personal digital assistants (PDAs), and IP Phones. Using the CTE with Cisco IP telephones in every room, guests have quick and easy access to hotel information (room service, in-house events), and third-party information (airline schedules, stock quotes, and weather information).

IP Centrex

This topic describes the IP Centrex implementations and applications.



Centrex service is regarded as an “outsourcing” of telephony call services. Centex does not maintain a PBX on customer premises. Instead, Centrex service removes the PBX function from the customer premises, provides a Centrex trunk to the customer, and provides the telephony services over the trunk. Typically, the Centrex trunk is arranged as a TDM channel associated signaling (CAS) circuit or as an ISDN Q.931 connection. Customer billing for this service is similar to the billing for outsourcing services.

IP Centrex performs the same job as a PBX but delivers the service over a packet network instead of a circuit-switched network. Service is accessed via an IP network and delivered to customers in a private or multitenant installation. The call control functions that Centrex delivers include:

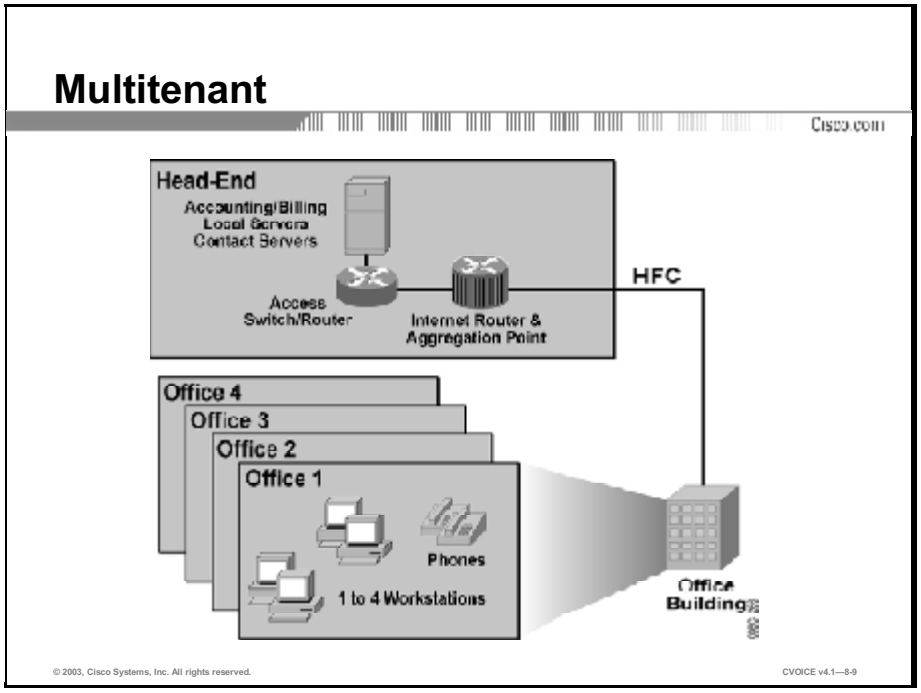
- Dial tone
- Interpretation of dialed digits
- Determination of called party status
- Call status return to caller, such as busy and ringback
- Call to voice-mail reroute, if applicable
- Billing services

Example

Cisco delivers IP Centrex through the use of a call agent, such as the Cisco BTS 10200 Softswitch. The figure illustrates the use of a call agent for the Centrex services that are delivered to telephones with the trunking gateway serving as a path to the PSTN.

Multitenant

This topic describes multitenant implementations and applications.



Multitenant applications allow building owners to deploy low-cost services, such as VoIP, cable television, and IP data services, to tenants in a common campus or building. Candidates for multitenant applications include:

- **Multi Dwelling Units (MDUs):** MDUs consist of high-rise and garden-style apartments, townhouses, and condominiums. Apartment renters and owners are now demanding high-speed Internet connections to home offices. Owners or MDU associations can attract new buyers or renters when they build an advanced cable IP infrastructure that offers secure, high-speed Internet access, cable television service, and VoIP access services.

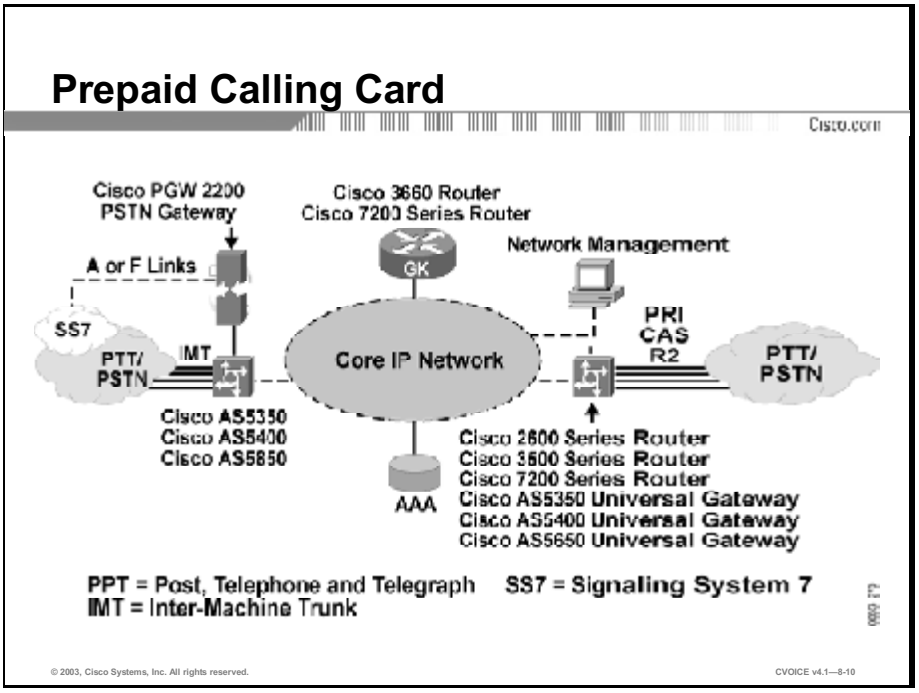
- **Multi-Tenant Units (MTUs):** MTUs are commercial properties that house a number of small or medium-sized offices. These users can leverage the existence of a cable IP infrastructure to:

  - Use a high-speed cable broadband medium for improved internal communications, which includes LAN services

  - Develop businesses, attract new opportunities, increase revenue streams through infrastructure advancements and services that support IP data and VoIP

Prepaid Calling Card

This topic describes the prepaid calling card implementations and applications.



Prepaid and postpaid calling-card services represent one of the fastest -growing types of enhanced voice services. A variety of consumer segments have propelled the growth of these services, including students, business and leisure travelers, expatriates, and immigrants. They are especially popular among mobile telephone users as an alternative to the costly international rates of mobile operators. For carriers who want to realize more profit from a global long-distance network, prepaid and postpaid calling-card services represent an opportunity to improve margins, direct minutes to the network, and increase customer retention. For service providers that are currently offering prepaid and postpaid calling-card services over a switched-circuit network, Cisco packet telephony networks provide a more cost-effective alternative for network expansions or upgrades.

Packet voice technology offers a compelling alternative to the traditional TDM switched-circuit network. Packet telephony networks reduce the cost and time-to-market requirements associated with launching or expanding voice services, such as national and international transport, voice mail and unified communications, text-to-speech, speech recognition, and calling card services. TDM-based services use a leased line and typically require a long-term financial commitment to that specific link. A TDM switch also represents a significant initial cash outlay and lengthy time period to achieve investment payback. The need to accelerate investment payback leads some providers to add fees for calling card activation or connection, diminishing the service marketability in the process.

Cisco offers a feature-rich solution for prepaid and postpaid calling-card services that is deployed via packet voice technology. The Cisco Voice Infrastructure and Applications (VIA) solution includes key features and attributes such as:

- A telephony user interface similar to PSTN card services applications
- Cost-efficiency in equipment and bandwidth
- Card recharging
- Balance transfer
- Personal identification number (PIN) change
- Support for multiple languages

The Cisco VIA solution offers the following benefits:

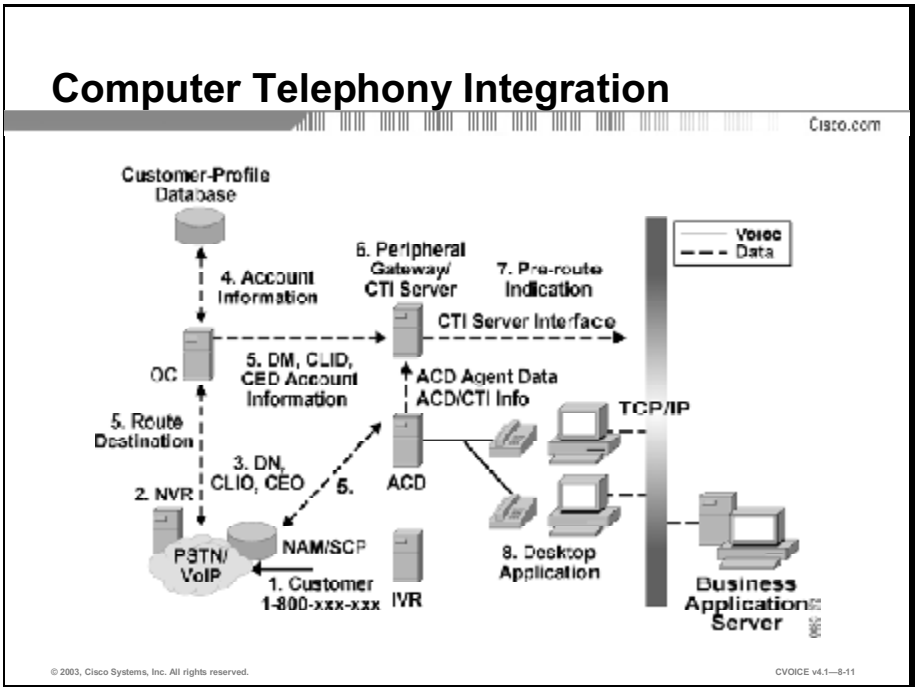
- Lower infrastructure and operating costs compared to other industry offerings
- Industry-leading voice quality, built-in reliability, and scalability
- Architectural and protocol flexibility
- Enables service providers of any size and location to compete in the calling card services market

Example

In the illustration, Cisco AS5XXX Access Servers allow calling-card customers into the network from the PSTN. The AAA (authentication, authorization, and accounting) server verifies the customer account status. When the account status is authorized, the gatekeeper directs the call across the IP core network, to the remote router or gateway, and connects to the PSTN. The service provider receives revenue for routing the call across the IP core, long distance.

Computer Telephony Integration

This topic describes implementation and application of computer telephony integration (CTI) systems.



CTI enables access to computer-processing functions while making, receiving, and managing telephone calls. CTI applications allow users to perform tasks such as retrieving customer information from a database of information provided by the caller ID. CTI applications also enable users to use the information captured by an interactive voice response (IVR) system to route a call to the appropriate customer service representative or to provide information to the individual receiving the call.

The following is a partial list of Cisco CTI applications:

- **Cisco IP SoftPhone:** Cisco IP SoftPhone, a desktop application, turns your computer into a full-feature telephone with the added advantages of call tracking, desktop collaboration, and one-click dialing from online directories. You can also use Cisco IP SoftPhone in tandem with a Cisco IP Phone to place, receive, and control calls from your desktop PC. All features function in both modes of operation.
- **Cisco IP Auto Attendant:** The Cisco IP Auto Attendant application works with Cisco CallManager to receive calls on specific telephone extensions and allow callers to select extensions.
- **Cisco WebAttendant:** Cisco WebAttendant provides a graphical user interface (GUI) for controlling a Cisco IP Phone to perform attendant console functions.
- **Personal Assistant:** Personal Assistant or a virtual secretary can selectively handle incoming calls and help users place outgoing calls.

Example

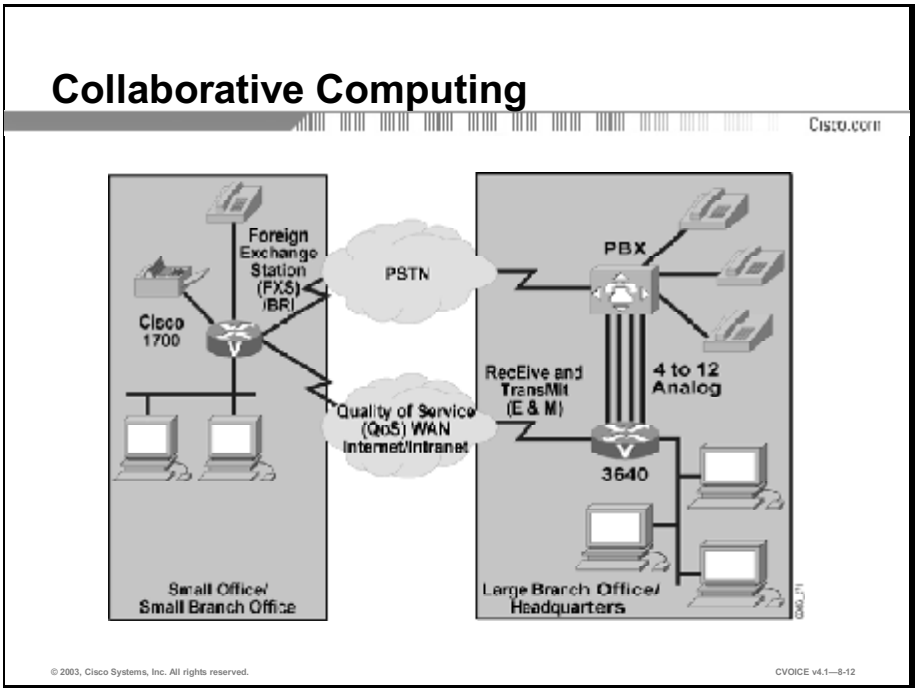
To illustrate how CTI works, consider a customer inquiry to a banking institution. The customer dials a toll-free telephone number from a home telephone. The agent who answers the call is in a pool of agents whose calls are delivered via an automatic call distributor (ACD). The preceding figure follows these steps:

1. The customer dials the toll-free number.
2. A Network Voice Response (NVR) system plays a script that collects caller-entered digits (CED), such as an account number.
3. The network sends a route request through an optical carrier (OC) interface to access the Customer-Profile Database.
4. The customer account information, CED, Dialed Number (DN), and calling line ID (CLID) are referenced in the Customer-Profile Database.
5. A route destination is returned to the Network Applications Manager/Service Control Point (NAM/SCP) and the DN, CLID, CED, and account information is forwarded to the automatic call distribution (ACD) system and peripheral gateway/CTI server.
6. The CTI server matches the selected agent from the ACD.
7. The CTI server sends a preroute indication across the CTI server interface to the TCP/IP network for pop-up delivery to the selected agent.
8. The TCP/IP network delivers the caller account information and CED information to the selected agent desktop.

Note The sample call data flow outlined above depicts an IVR in the carrier network. Alternatively, prompting may occur through an IVR at the premises or through a combination of network and premises-based IVRs.

Collaborative Computing

This topic describes the collaborative computing implementations and applications.



Collaborative computing allows team members, on a shared project, to share resources and applications “in real time” regardless of their physical location. The figure illustrates a simple VoIP internetwork that allows collaborative computing. The PSTN serves as a gateway to non-enterprise connected participants.

At the heart of the collaborative computing solution is the IP internetwork. Participants connect to each other via a private IP network or the public Internet. Servers and applications are deployed across the network, including the client software on the participant desktops. Collaborative computing applications include:

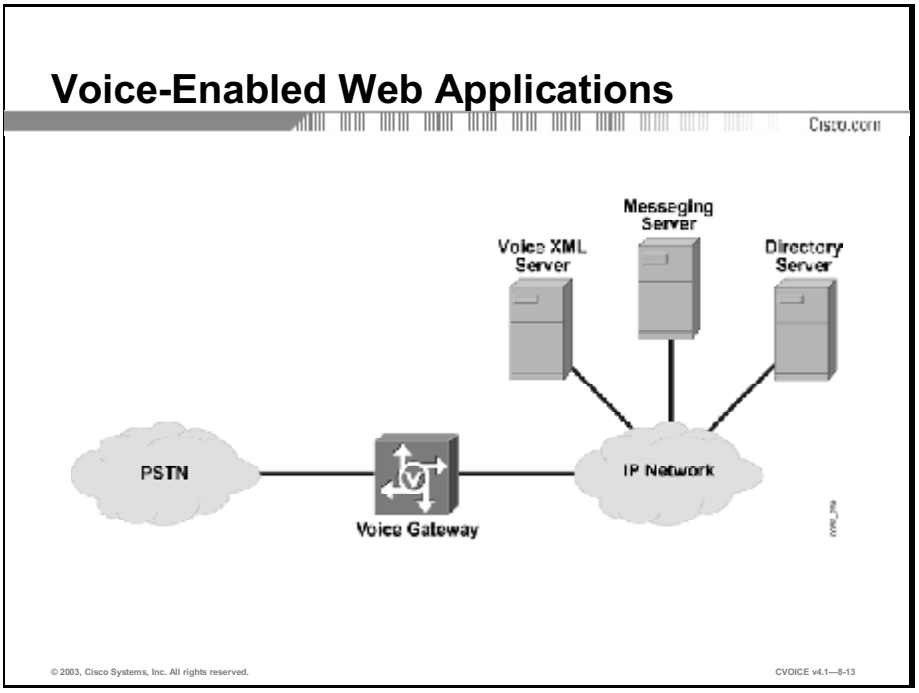
- Telephony and meeting applications, such as Microsoft NetMeeting
- Scheduling and collaboration software, such as IBM Lotus Notes
- Video streaming software
- FTP, TFTP, and peer-to-peer file sharing applications
- IP Phones
- Whiteboard software

The goals of collaborative computing include:

- Reduced travel expenses
- Network transparency
- Shared calendar
- Real-time document sharing
- Real-time contact, such as telephony or videoconferencing

Voice-Enabled Web Applications

This topic describes the implementation and application of voice-enabled web applications.



Cisco AS5400 Series Universal Gateways can interpret Voice Extensible Markup Language (VoiceXML) documents. VoiceXML is an open-standard markup language that creates voice-enabled web browsers and IVR applications. While HTML enables users to retrieve data with a PC, VoiceXML enables subscribers to retrieve data with a telephone. The universal accessibility of the telephone and its ease of use make VoiceXML applications a powerful alternative to HTML for Internet access. The Cisco VoiceXML solution infrastructure takes advantage of Cisco AS5400 Series Universal Gateway domain specific part (DSP) resources, signaling, and media conversion capabilities to execute VoiceXML application logic at the edge of the network, on offloading servers, and within the network to support unified communications services.

Example

Consider the following scenario:

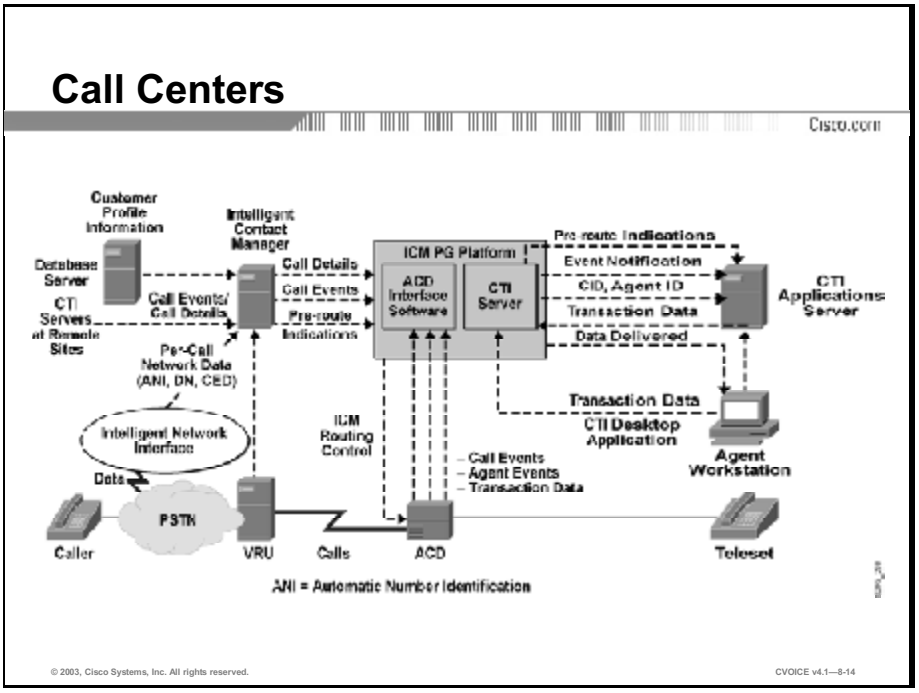
1. A baseball fan dials a number from the PSTN and is connected to a Cisco Voice Gateway that is configured as a VoiceXML-enabled gateway.
2. The Cisco Voice Gateway uses the caller ID information and associates it with the appropriate VoiceXML document that resides on a web server. This document provides baseball scores for the caller.

3. The voice gateway runs the VoiceXML document and responds to the caller by playing the appropriate audio content. The application might play a recorded prompt that asks the caller to press a specific dual-tone multifrequency (DTMF) key to hear a sports score, such as, “Press 2 to hear the results of playoff game between Baltimore and New York.”

4. Cisco IOS® VoiceXML can transfer the caller to another party, such as customer service; for example, after playing the score, the application might prompt the caller with the message, “If you sign up for a one-year subscription to this service now, you will be entered into a drawing for two tickets to the next World Series. Press 5 to speak to one of our agents.”

Call Centers

This topic describes the call center implementations and applications for VoIP.



Call centers are the hub of the customer service efforts of many growing businesses. Forward-thinking companies are integrating this key function with Internet technology to transform customer care into a powerful business-building force.

Firms such as catalog sellers, telemarketers, and computer helpdesks use traditional call centers to manage large volumes of telephone calls and customer contacts. Call center applications route incoming calls to sales and service agents who can respond to customer needs. Integrating this call center activity with an Internet-based customer relationship management (CRM) solution gives agents immediate access to customer purchase histories, order tracking capabilities, and other key information and tools. This enhanced information flow enables call-center staff to use customer interaction to build customer loyalty and retention.

Traditional call center technology recognizes incoming calls and routes them to available agents. These call center technologies include recognition of customer telephone numbers, account numbers, or IDs. Customer data appears on the agent computer screen, ensuring that the agent can access the customer orders, account balance, and other crucial data. However, real-time collaboration between the customer and the agent is limited to the spoken word. Demonstrative services and offers of product are limited to verbal description, usually a script read by the agent.

Cisco IP Contact Center (IPCC) with Internet access allows call center agents to respond to customer queries over a variety of channels, such as telephone, e-mail, web, and fax.

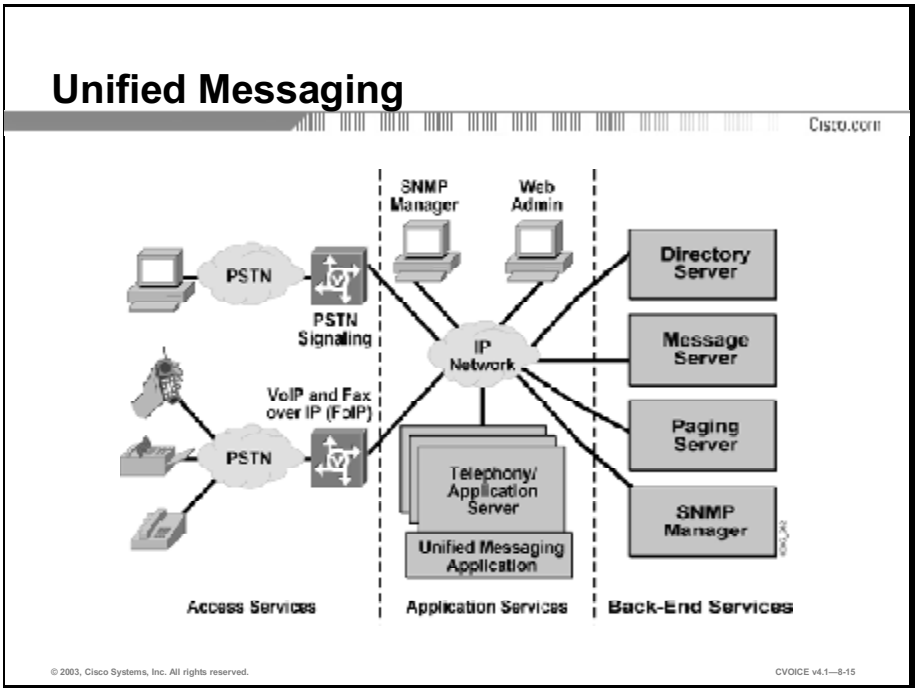
Example

When a customer calls with questions about a new product, an agent can immediately send an e-mail message that includes product specifications and a link to a downloadable interactive demo. This scenario allows customer-service agents to take on sales and marketing roles, which helps the company roll out new initiatives and promotions quickly to targeted customers. Other ways to enhance real-time customer collaboration include FAX-back services and web-page collaboration, where the customer and agent interact on the same web page to ensure, for example, that the color of a sweater is correct.

Call centers use a range of telephone, computer, and network technologies, including VoIP. In the preceding figure, Cisco Intelligent Call Management (ICM) software is at the heart of the call center application. The ICM uses computer telephony integration (CTI) technology to deliver caller account information to the agent desktop while the agent receives the VoIP call. The location independence of the agents adds another benefit to this model. “Follow-the-sun” customer support programs allow 24/7 customer service, regardless of the location of the agents.

Unified Messaging

This topic describes the unified messaging (UM) system implementations and applications.



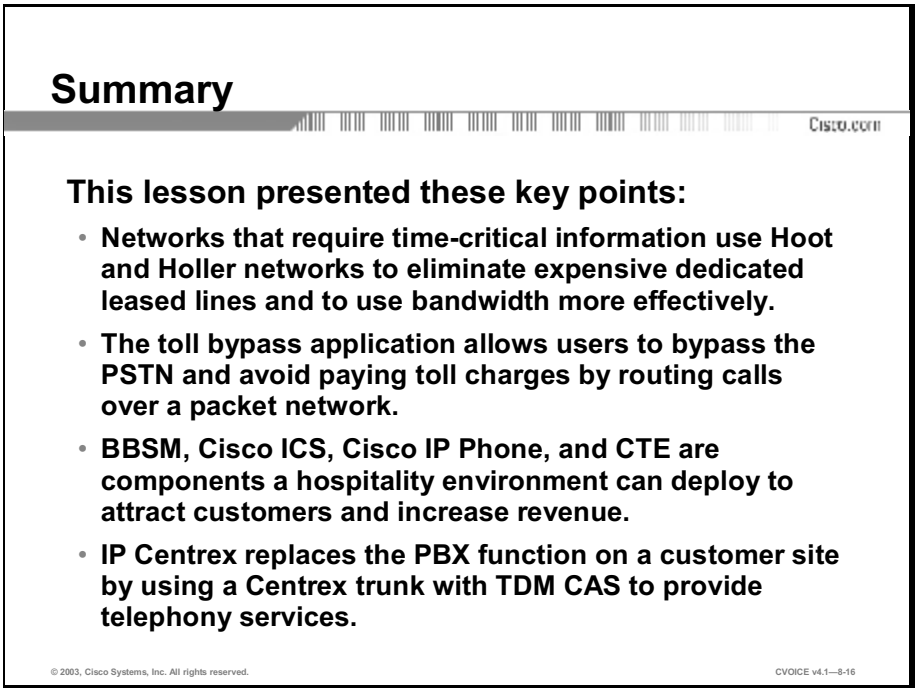
Cisco Unity is designed for an IP environment and complements the full range of IP Communications solutions—such as Cisco CallManager, Cisco Personal Assistant, and Cisco IP Contact Center. Cisco Unity provides advanced capabilities that unify data and voice. Cisco Architecture for Voice, Video and Integrated Data (AVVID) enables Cisco Unity to provide a solid foundation to roll out future convergence-based communications services. It is less expensive to use IP for a comprehensive communications solution deployment because it is a single network for both voice and data.

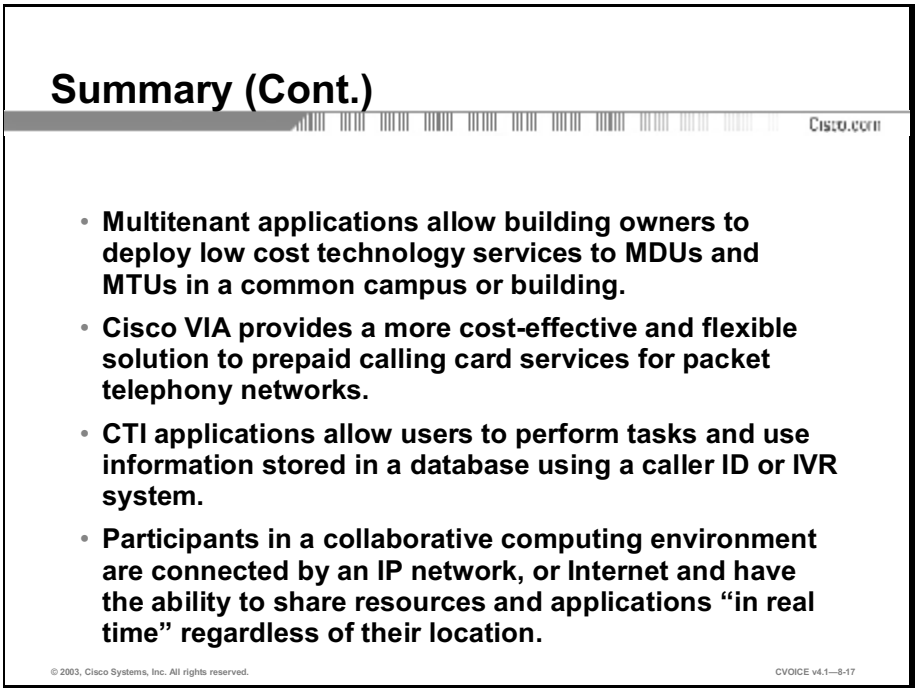
Cisco Unity leverages existing communications infrastructure investments by integrating with leading legacy PBXs and interoperating with legacy voice-mail systems. Cisco Unity supports legacy PBX systems and Cisco CallManager—even simultaneously—paving the way for a cost-effective migration to full IP telephony. Cisco Unity has an optional Audio Messaging Interchange Specification-A (AMIS-A) networking module that allows message interchange between disparate voice messaging systems that support this industry-standard messaging protocol. Cisco Unity Bridge enables advanced message interchange functionality with Avaya and Octel voice messaging systems. With AMIS-A and Cisco Unity Bridge, customers that deploy Cisco Unity can continue to use their legacy messaging systems, to ensure a smooth transition.

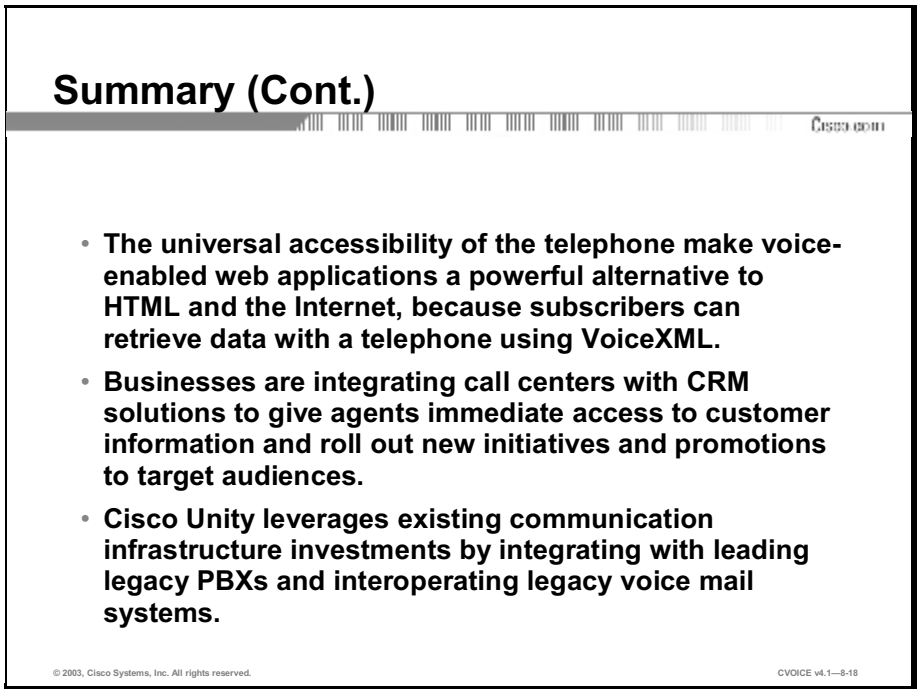
Because Cisco Unity shares the same directory as the exchange network, users can make subscriber moves, adds, and changes from one place, eliminating redundant tasks. Studies show that the average cost of a typical system move, addition, or change to a user account is between $75 and $100. Eliminating duplicate administration for separate voice and e-mail systems can quickly pay for the entire system. In addition, because all messages are housed in the same message store, backup costs are cut in half.

Summary

This topic summarizes the key points discussed in this lesson.







Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Applications

References

For additional information, refer to these resources:

- "Multicast Hoot 'n' Holler"
  http://www.cisco.com/warp/public/cc/so/neso/vvda/hthllr/hhoip_wp.htm
- "MGCP Basic CLASS and Operator Services"
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcpgr.htm
- "Service Overview Prepaid and Postpaid Call Card Services"
  http://www.cisco.com/warp/public/cc/so/neso/voso/ns68/ppccs_ov.htm
- "Cisco VoiceXML Solution Infrastructure"
  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/vxml_uc/vxml_rn.htm

Quiz: Applications

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Describe the types of networks that implement Hoot and Holler networks and list two reasons businesses may choose this method of networking
- Explain how enterprise customers can avoid paying toll charges when making interoffice calls
- List the four components a hospitality enterprise can provide and explain the value it can bring to their business
- Explain how an IP Centrex can replace a PBX on a customer site and describe the services it provides
- List two candidates for multitenant applications and explain why building owners are beginning to build this type of network
- Describe the features and benefits of Cisco Voice Infrastructure and Applications, when using prepaid calling card services in a packet telephony network
- Describe the purpose of a CTI system and describe how it is accessed
- Describe how participants in a collaborative computing environment are connected and the benefit of this type of connection
- Explain how voice-enabled web applications work and why they are an alternative to the Internet
- Explain how call centers are changing to meet the needs of customers
- Describe how the Cisco brand of unified messaging system is used in an IP environment

Instructions

Answer these questions:

Q1) Hoot and Holler requires that _____ be enabled on the router.

A) SPRT

B) IP Multicast

C) IGRP

D) IGMP

Q2) Which modern technology have Hoot and Holler systems evolved into?

A) dial-on-demand

B) Advanced Peer-to-Peer Networking

C) B-ISDN

D) specialized leased-line

Q3) Toll bypass allow some ISPs to offer residential customers free or very low-cost _____.

A) Internet Access

B) software

C) long distance voice calls

D) bundled services

Q4) When customers are using toll bypass, which type of network is used for their long-distance voice calls?

A) PSTN with TDM-based switches

B) packet network with routers

C) PSTN with edge voice gateways

D) packet network with TDM-based routers

Q5) In the case of a hotel, a building or campus is wired with a _____ to supply voice, video, and Internet applications to the guest room.

A) LAN

B) ATM

C) 802.11 network access points

D) single broadband access line

Q6) Which two Cisco applications would you implement to provide hotel guests with access to room service and in-house events as well as airline flight status and weather updates? (Choose two.)

A) BBSM

B) Cisco IP Phone

C) Cisco ICS

D) CTI

E) CTE

F) Cisco IP AutoAttendant

Q7) Centrex is regarded as a(n) _____ of telephony call services.

A) outdated mode

B) outsourcing

C) outplacement

D) outside network

Q8) Which two call control functions are provided by Centrex? (Choose two.)

A) billing services

B) CAC

C) authentication and authorization

D) RTP

E) dial tone

Q9) Which services can building owners deploy using multitenant applications?

A) VoIP

B) cable television

C) IP data services

D) all of the above

Q10) Multitenant applications allow building owners to deploy low-cost services to tenants in a common _____.

A) area code

B) ATM Infrastructure

C) campus or building

D) television viewing area

Q11) The Cisco VIA solution includes two key features and attributes such as _____ and _____. (Choose two.)

A) card recharging

B) sports scores

C) balance transfer

D) paging

E) automatic redial

Q12) Which type of network offers the least expensive option for prepaid and postpaid calling card services?

A) switched-circuit network

B) TDM-based network

C) packet voice network

D) none of the above

Q13) CTI applications allow users to perform tasks such as retrieving customer information from a database based on information provided by the _____.

A) caller ID

B) CTI server

C) amateur radio network

D) satellite system

Q14) Which CTI application can selectively handle incoming calls and help users make outgoing calls?

A) Cisco IP SoftPhone

B) Cisco IP AutoAttendant

C) Cisco IP Phone

D) Cisco WebAttendant

E) Personal Assistant

Q15) Two collaborative computing applications include _____ and _____. (Choose two.):

A) Microsoft Excel

B) Microsoft NetMeeting

C) Linux 7.3

D) IBM Lotus Notes

E) HTML applications

Q16) What is the function of collaborative computing?

A) allows team members to interact on a web page

B) allows team members in the same physical location to share resources and applications

C) allows team members to share resources and applications “in real time” regardless of their physical location

D) allows team members to develop spreadsheet applications such as Microsoft Excel

Q17) Which type of documents can Cisco AS5400 Series Universal Gateways interpret?

A) HTTP

B) WordStar

C) text

D) VoiceXML

Q18) At what location in the network does Cisco AS5400 Series Universal Gateways execute VoiceXML application logic to provide unified communications services?

A) the edge of the network

B) on offloading servers

C) within the network

D) all of the above

Q19) Which service is NOT offered by traditional call center technology?

A) recognition of customer telephones

B) recognition of customer ID

C) ability to view customer data while on the call

D) ability to access customer account balance while on the call

E) ability to send e-mail to the customer while on the call

Q20) Which Cisco application with Internet access allows call center agents to respond to customer queries over a variety of channels?

A) Cisco IPCC

B) Cisco IVR

C) Cisco IP Phone

D) Cisco AS5400 Series Universal Gateways

Q21) Which legacy devices does Cisco Unity integrate with in order to leverage existing communications infrastructure investments?

A) desktops

B) routers

C) trunks

D) PBXs

Q22) Which feature of Cisco Unity allows message interchange between disparate voice messaging systems?

A) Cisco Unity Bridge

B) AMIS-A

C) Avaya

D) Octel

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent.

E

Laboratory Exercises

This appendix contains the following laboratory exercises:

- Laboratory Exercise 2-1: Lab Familiarity
- Laboratory Exercise 3-1: Voice Port Configuration
- Laboratory Exercise 4-1: Plain Old Telephone Service Dial Peers
- Laboratory Exercise 4-2: Connections
- Laboratory Exercise 5-1: Basic Voice over IP
- Laboratory Exercise 6-1: Voice over IP with H.323
- Laboratory Exercise 6-2: Voice over IP with SIP
- Laboratory Exercise 6-3: Voice over IP with Media Gateway Control Protocol
- Laboratory Exercise 7-1: Quality of Service
- Laboratory Exercise 7-2: Call Admission Control

Laboratory Exercise 2-1: Lab Familiarity

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

Each pod contains two complete sets of hardware and a shared public switched telephone network (PSTN) simulator.

These are the resources and equipment each pod requires to complete this exercise:

- Two voice-enabled routers
- Two client/servers (laptop or desktop computers)
- Two Ethernet crossover cables
- Three serial crossover (DTE-DCE) cables

Exercise Objective

In this exercise, you will become familiar with the routers in your pod and your pod's relationship with the other pods. You will also personalize your pod's 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 exercise, you will be able to:

- 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

Command List

The commands used in this exercise are described in the table here.

Table 1: Exercise Commands

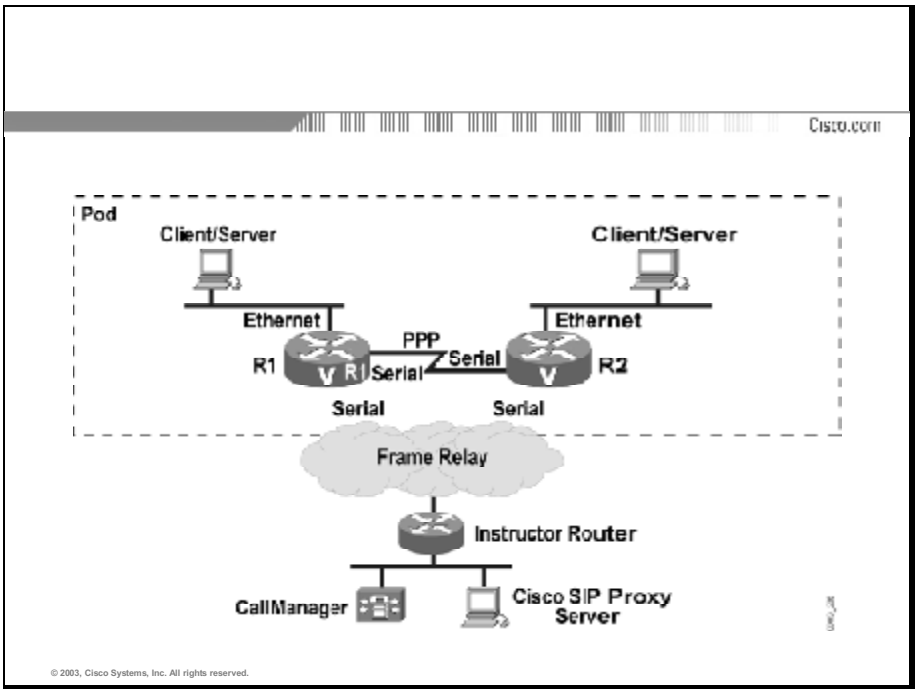
Command	Description
clock rate *rate*	Configures the clock rate for the hardware connections on serial interfaces. This command is executed in interface configuration mode.
configure terminal	Enters configuration mode. This command is executed in privileged mode.
copy running-config startup-config	Copies current running configuration into NVRAM. This command is executed in privileged mode.
enable	Enters privileged mode. This command is executed in user mode.
enable secret *password*	Sets password to control access to privilege level. This command is executed in global configuration mode.
encapsulation *encap-type*	Sets the encapsulation type. This command is executed in interface configuration mode.
hostname *name*	Assigns a name to the router. This command is executed in global configuration mode.
interface [Ethernet,serial] *n*	Enters interface configuration mode for the specified interface. This command is executed in global configuration mode.
ip address *ip-address mask*	Configures the IP address and mask. This command is executed in interface configuration mode.
ip host *hostname ip-address*	Creates an IP host table entry assigning a name to an IP address. This command is executed in global configuration mode.
line vty 0 4	Enters vty line configuration mode for lines 0 through 4. This command is executed in global configuration mode.
logging synchronous	Redisplays the current line after a logging message has been displayed onscreen. Use for console or vty lines for cleaner display.
login	Enables password checking at login. This command is executed in line configuration mode.
network *network-address*	Specifies a list of networks for the Enhanced Interior Gateway Routing Protocol (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 *password*	Sets a password. This command is executed in line configuration mode.
ping (*ip-address or host name)*	Tests the reachability of a device. When in user mode, it 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 *as-number*	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 config, 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, as well as where routing breaks down. When in user mode, it 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 laboratory exercises.

Lab Diagram



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 following table contains evidence of the following 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, nonbroadcast multiaccess (NBMA) network using network 192.168.1.0.

In addition, the instructor's Ethernet uses addresses in network 192.168.100.0.

Table 2: 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

Table 3: Hostname Table

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

Exercise Procedure

Complete these steps:

Step 1 Using the client/server, connect to the console port of your router.

Step 2 Identify the 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 below:

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 below:

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/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/router. For the PPP connection between the voice-enabled routers in the pod, configure R1 to be the DTE side and R2 the DCE side of the connection.

R1	Interface Number	IP Address	DTE/DCE
PPP Serial			
Frame Serial			
Ethernet			N/A
Frame Switch		N/A	

Step 6 Configure your router host name with the appropriate name from the Hostname Table. 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 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.

Step 10 Enable EIGRP routing for Autonomous System 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.

Exercise Verification

You have completed this exercise when you attain these results:

- See all other classroom subnets in your IP routing table
- Trace or ping from your client/server to all other client/servers in the classroom

Laboratory Exercise 3-1: Voice Port Configuration

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment each pod requires to complete this exercise:

- Two T1 crossover cables
- Two PBX devices
- Four telephones
- Four RJ-11 cables

Exercise Objective

In this exercise, 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 exercise, you will be able to:

- Identify default voice port settings
- Customize and verify analog port operations
- Create, customize, and verify digital port operations

Command List

The commands used in this exercise are described in the table here.

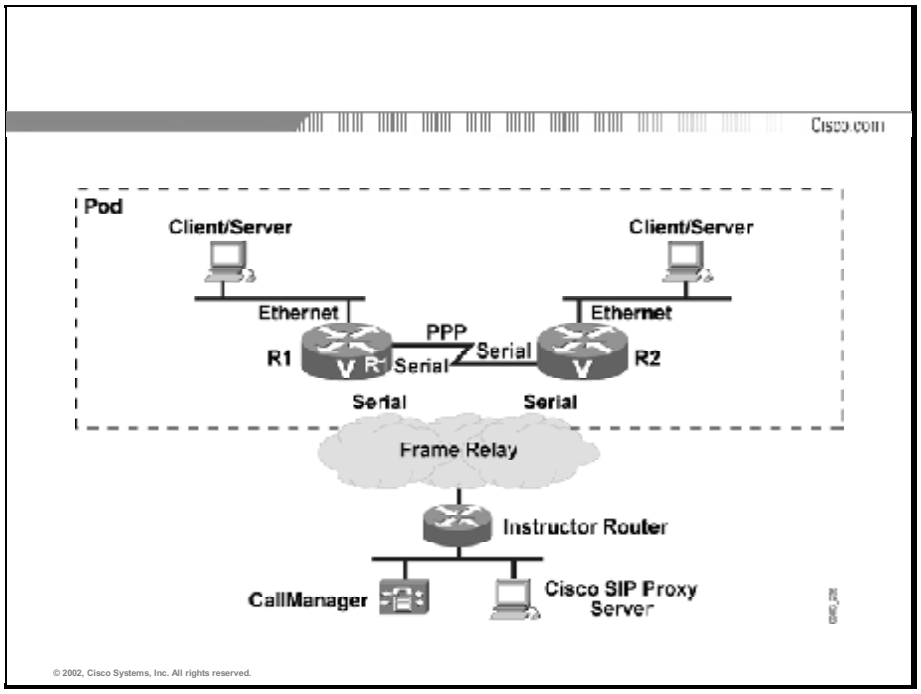
Table 1: Voice Port Commands

Command	Description
clock source ***source***	Specifies the clock source. This command is executed in controller configuration mode.
controller t1 ***n***	Enters T1 controller configuration mode for the specified controller. This command is executed in global configuration mode.
cptone ***country-code***	Sets the regional analog voice interface–related tone, ring, and cadence setting. This command is executed in voice-port configuration mode.
default ***parameter***	Resets the value of the parameter to its default value. This command is executed in multi mode.
ds0-group ***tag*** **timeslots** ***timeslot-list*** **type** ***signaling-type***	Specifies the DS0 time slots 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.
framing ***sf*** | ***esf***	Specifies the framing type. This command is executed in controller configuration mode.
linecode ***ami*** | ***b8zs***	Specifies the line code setting. This command is executed in controller configuration mode.
ring cadence define ***pulse interval***	Sets the ring cadence for the Foreign Exchange Station (FXS) port. This defines how the phone will ring. This command is executed in **voice-port** command.
show voice port (summary)	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.
timeouts initial ***secs***	Sets the number of seconds for which the system will wait for the caller to input the first digit. This command is executed in voice-port configuration mode.
voice-port ***port-number***	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 laboratory exercise(s).

Lab Diagram



PBX Configuration

PBX parameters are as follows:

- T1 connection
- Timeslots 1–24
- Ear and mouth (E&M) Wink-Start signaling
- Clock source is line
- Extended Superframe (ESF) framing
- B8ZS line code

Task 1: Analog Voice Port Configuration

In this task, you will examine analog voice ports and configures voice-port parameters.

Exercise 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 the router is powered on and the cable is firmly seated. If the problem persists, ask your instructor for help.

Step 3 Using **show** commands, identify available voice ports, their type, and their default settings. Record the information below:

	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 Since many companies have international offices, it is important to know how to configure the voice port to match that country's standard signaling. For this step, assume you are configuring this router for Australia. On the FXS port that your phone 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 below:

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 phone 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 Since you will be working with two telephones all week, you may want one phone 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 out in the next lab. What ring cadence did you define? _____

Exercise Verification

You have completed this exercise when you attain these results:

- Configure and verify 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.

Exercise 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 below:

Framing _____

Line code _____

Clock source _____

Step 3 Configure your T1 controller to match the settings of the PBX as shown in the Job Aids section. Remember that since 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 match 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 below:

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.

Exercise Verification

You have completed this exercise when you attain these results-:

- Verify the T1 connection to the PBX
- Verify the existence of the newly created digital voice port

Laboratory Exercise 4-1: Plain Old Telephone Service Dial Peers

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment each pod requires to complete this exercise:

- One PSTN device
- One telephone
- One RJ-11 cables

Exercise Objective

In this exercise, you will configure plain old telephone service (POTS) dial peers to establish locally terminated calls, calls through a private branch exchange (PBX), and calls to the public switched telephone network (PSTN). You will also experiment with two different configurations to control hunt capabilities.

After completing this exercise, you will be able to:

- Configure dial peers for locally terminated calls, PBX calls, and PSTN calls
- Determine appropriate methods of digit forwarding and manipulation
- Create hunt groups and determine hunting behavior

Command List

The commands used in this exercise are described in the table here.

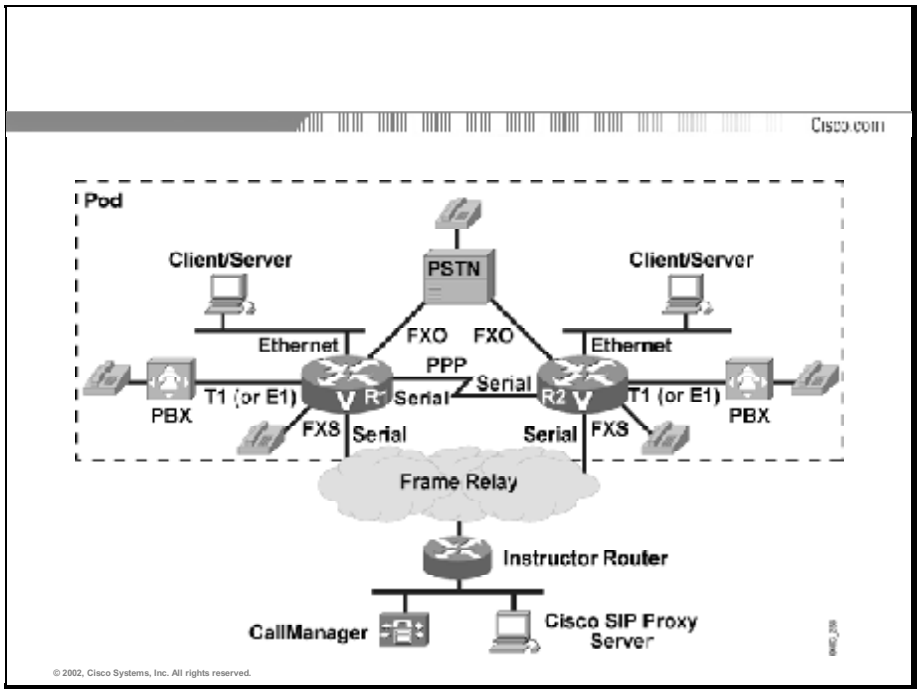
Table 1: Dial Peer Commands

Command	Description
debug vpm signal	Displays real-time Voice Processor Module signaling. This command is executed in privileged mode.
debug vtsp dsp	Displays digits as they are received by the voice port. This command is executed in privileged mode.
destination-pattern *string*	Configures a telephone number for this dial peer. This command is executed in dial-peer configuration mode.
dial-peer hunt *0-7*	Specifies a hunt selection order for dial peers. This command is executed in global configuration mode.
dial-peer voice *tag* **pots**	Enters dial-peer configuration mode. This command is executed in global configuration mode.
forward-digits	Specifies which digits to forward for voice calls. This command is executed in dial-peer configuration mode.
port *port-number*	Configures the port for this dial peer. This command is executed in dial-peer configuration mode.
preference *0-9*	Specifies the preferred order of a dial peer within a hunt group. This command is executed in dial-peer configuration mode.
show call active voice	Displays information on active calls. This command is executed in user mode.
show dial-peer voice (*tag***) | (summary)**	Displays dial-peer configuration information. This command is executed in user mode. The **summary** option is available in privileged mode only.
show dialplan number *number*	Displays which dial peer is matched when a particular telephone number is dialed. This command is executed in privileged mode.
show voice call summary	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 laboratory exercise:

Lab Diagram



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:

- 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.

Table 2: Classroom Dial Plan

Pod Number		1	2	3	4	5	6
R1		1101 1102	2101 2102	3101 3102	4101 4102	5101 5102	6101 6102
PBX1		1151	2151	3151	4151	5151	6151
R2		1201 1202	2201 2202	3201 3202	4201 4202	5201 5202	6201 6202
PBX2		1251	2251	3251	4251	5251	6251
PSTN	Port 1 Port 2 Port 3	555-1001 555-1002 555-1003	555-2001 555-2002 555-2003	555-3001 555-3002 555-3003	555-4001 555-4002 555-4003	555-5001 555-5002 555-5003	555-6001 555-6002 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.

Exercise Procedure

Complete these steps:

Step 1 Using Table 2 in the Job Aids section, verify the telephone numbers you will use for your local telephones. Note these numbers below:

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 configuration.

Step 3 Use 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 the following 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 **debug** 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.

Exercise Verification

You have completed this exercise when you attain these results:

- Call between your locally terminated telephones in both directions.

Task 2: Forward Calls to the PSTN

In this task, you will configure appropriate ports and dial peers to place calls to the PSTN. Initially this will be done with two-stage dialing, meaning 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.

Exercise Procedure

Complete these steps:

Step 1 Connect the PSTN device to each of the pod's routers using RJ-11 cables. Connect a single telephone to the PSTN device. Answer the following questions:

a) Which voice port type did you connect to the PSTN?_____

b) What is the port number?_____

c) What is the phone number of your PSTN port?_____

d) What is the phone number of your partner's PSTN port?_____

e) What is the phone number of the PSTN-connected telephone?_____

Step 2 In this scenario, the requirement is to dial 9 to reach the PSTN. Configure dial peers to allow calls to the PSTN. 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 to forward 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?_____

What command did you use to forward digits to the PSTN? _____

What other method could you have used?_____

Exercise Verification

You have completed this exercise when you obtain these results:

- Place 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.

Exercise 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 below:

Hunt group number _____

Step 2 Ensure that both telephones are still connected to your router voice ports.

Step 3 Configure additional dial peers to reach both voice ports using the same new hunt group number for each dial peer. Do not edit existing dial peers for this exercise, as they will be needed for future labs.

Step 4 To properly test the hunt behavior between your two phones, you will use the PSTN phone. To reach the hunt group number, dial the 7-digit PSTN number of the port that attaches to your router. At the secondary dial tone, dial your hunt group number. Take note of any patterns as to how calls are allocated to each phone. 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?_____

Step 6 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 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 7 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 below.

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?

Exercise Verification

You have completed this exercise when you attain these results:

- 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.

Exercise Procedure

Complete these steps:

Step 1 Move one of your telephones and plug it into the lowest numbered port of your PBX device. Since 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 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.

Exercise Verification

You have completed this exercise when you attain these results:

- Call in both directions between the PBX-attached telephone and the router-attached telephone.

Laboratory Exercise 4-2: Connections

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- No new resources are required.

Exercise Objective

In this exercise, you will explore different connection types and their uses.

After completing this exercise, you will be able to:

- Simulate autoattendant functions through use of private line, automatic ringdown (PLAR) and PLAR off-premises extension
- Create a tie-line connection for calls between two PBXs
- Use appropriate **show** and **debug** commands to monitor and troubleshoot the connections

Command List

The commands used in this exercise are described in the table here.

Table 1: Connection Commands

Command	Description
connection plar opx ***string***	Specifies PLAR off-premise extension connection. This command is executed in voiceport config mode.
connection plar ***string***	Specifies a PLAR connection. This command is executed in voiceport config mode.
connection tie-line ***string***	Specifies a tie-line connection. This command is executed in voiceport config mode.

Task 1: Connecting to PLAR and PLAR OPX

By default, when a call comes into a Foreign Exchange Office (FXO) port, the router presents dial tone after going off-hook to answer the call. At times this default behavior may not be desirable. You will configure the voice port to simulate an autoattendant function in this section.

Exercise Procedure

Complete these steps:

Note	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 labs configuration.

Step 1 You will simulate an autoattendant by configuring PLAR on the FXO port of your voice-enabled router. You will direct all calls coming into the FXO port to the telephone connected to your Foreign Exchange Station (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 to the ringback tone. You should hear an initial ringback from the PSTN, then a secondary ringback from the FXS port as it is ringing the telephone. From the PSTN's perspective, the call is complete and billing has started.

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? _____

Exercise Verification

You have completed this exercise when you attain these results:

- Place a call to the FXO port of your router from the PSTN-attached telephone and, without further dialing, connect to the router-attached telephone.
- Explain the difference between PLAR and PLAR OPX.

Task 2: Connection Tie-Line

In the previous task, 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 connected two PBXs together when a user at one site needed 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.

Exercise Procedure

Complete these steps:

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 Voice over IP (VoIP) dial peer to point the call across the network toward your partner's PBX. Since there is no loopback address, you can use any valid address on your partner's router to send the call to.

Write your partner's IP address here _____

Ping it 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 your partner's PBX-attached telephone? _____

What five-digit number will the router process to connect to your partner's PBX-attached telephone? _____

Step 3 To complete the tie-line connection across the IP network, you will have to enter the following VoIP dial peer:

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 the last task, remember that your partner will be calling your PBX-attached telephone as well. Your partner's router will be passing a five-digit string to your router to complete the call to your PBX.

What five-digit string will your partner's router be passing to your router for calls destined to your PBX telephone? _____

Configure a plain old telephone service (POTS) dial peer to terminate the five-digit string as it comes in from your partner's 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**.

Exercise Verification

You have completed this exercise when you attain these results:

- Configure and verify tie-line connections between PBXs.
- Place calls in both directions between PBX-attached telephones.

Laboratory Exercise 5-1: Basic Voice over IP

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- No new resources are required.

Exercise Objective

In this exercise, you will establish basic Voice over IP (VoIP) connectivity between telephones in your pod. You will also investigate the use of appropriate VoIP dial peer parameters.

After completing this exercise, you will be able to:

- 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

Command List

The commands used in this exercise are described in the table here.

Table 1: VoIP Commands

Command	Description
codec *codec-name*	Specifies which codec is to be used for calls matching this dial peer. This command is executed in dial-peer configuration mode.
codec preference *1-14 codec-name*	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 class configuration mode.
debug voip ccapi inout	Displays real-time call control processing and call leg information. This command is executed in privileged mode.
debug voip rtcp	Displays real-time RTCP reports per call. This command is executed in privileged mode.
default *parameter*	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.
dial-peer voice *tag* **voip**	Enters dial-peer configuration mode and specifies VoIP. This command is executed in global configuration mode.
frame relay ip rtp header-compression	Enables RTP header compression on a Frame Relay interface. This command is executed in interface configuration mode.
ip rtp header-compression	Enables RTP header compression on an interface. This command is executed in interface configuration mode.
session target ipv4:*x.x.x.x*	Specifies the destination IP address for the gateway terminating a VoIP call. This command is executed in dial-peer configuration mode.
show voice dsp	Displays DSP usage. This command is executed in user mode.
show ip rtp header-compression	Displays statistics relating to RTP header compression. This command is executed in user mode.
voice class codec *tag*	Enters voice class codec configuration mode. This command is executed in global configuration mode.
voice-class codec *tag*	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 Aids

These job aids are available to help you complete the laboratory exercise:

- Understanding **debug voip ccapi inout** command output. (See sample output after Task 4.)

Task 1: VoIP Dial Peers

You will start this lab 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 your partner's telephones.

Exercise Procedure

Complete these steps:

Step 1 Configure VoIP dial peers to reach both the router-attached telephone and the PBX-attached telephone connected to your partner's equipment. In preparation, note your partner's two telephone numbers below. Also note a valid IP address on your partner's router.

Telephone numbers:_____ _____

IP address:_____

Step 2 Test your configuration by placing calls to both of your partner's telephones.

Step 3 Use **show** commands to verify:

- Which dial peer will be matched when a specific number is dialed
- Active call parameters
- What digital signal processor (DSP) resources are being used for the call

Step 4 Use **debug** commands to verify:

- What the calling number is
- What the called number is
- Which dial peer was matched

Step 5 Use the **debug voip rtcp** command to view the control protocol information being reported for the call.

Exercise Verification

You have completed this exercise when you attain these results:

- Place calls to both of your partner's telephones.

Task 2: Codec Configuration

You will change the codec settings on your VoIP dial peers and investigate how it impacts 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 perform tests together.

Exercise Procedure

Complete these steps:

Step 1 Use **show** commands to verify the default codec setting and note it below.

Default codec:_____

Step 2 Change the codec on R1's 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 R2's VoIP dial peer pointing to R1 to match R1's codec.

Step 5 Verify whether the codec was successful, and if so, which codec was used.

Was the call successful?_____ Codec used _____

Exercise Verification

You have completed this exercise when you attain these results:

- Successfully configure the codec setting for VoIP calls.

Task 3: Effects of Bandwidth Requirements and Header Compression

You will investigate the effects of passing voice over low bandwidth links and the tools available to improve voice quality on those links.

Exercise Procedure

Complete these steps:

Step 1 Using the bandwidth requirement concepts, determine the required bandwidth for a G.711 call without header compression on: PPP link_____ Frame Relay Link _____

Step 2 Change the codec on both R1 and R1 to g711ulaw. Place a call from one router-connected telephone to the other 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.

What command did you use on the PPP link?_____

What command did you use on the Frame Relay link?_____

Step 4 Test the voice quality. Has the quality improved? Why or why not? Is it acceptable?

Step 5 Change the codec on both R1 and R2 back to the default setting. What command did you use to reset to the default?_____

Exercise Verification

You have completed this exercise when you attain these results:

- Explain how and when to use RTP header compression

Task 4: Configuring CODEC Negotiation

As you saw in the previous sections, 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 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. In order for a single dial peer to match more than one codec, you must configure a list of codecs to negotiate.

Exercise 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 your partner's IP address.

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.

Exercise Verification

You have completed this exercise when you attain these results:

- Explain how and when to configure codec negotiation parameters

Debug voip ccapi inout Command Output Sample

```
The primary command to debug end-to-end VoIP calls is debug voip
ccapi inout. The output from a call debug is shown below. !-- Action:
A VoIP call is originated through the Telephony SPI (pots leg) to
!-- extension 5000.  <some output has been omitted>


maui-voip-austin#debug voip ccapi inout
voip ccAPI function enter/exit debugging is on


!-- Call leg identification, source peer: Call originated from dial-
peer 1 pots
!-- (extension 4000)


*Mar 15 22:07:11.959: cc_api_call_setup_ind (vdbPtr=0x81B09EFC,
callInfo={called=, calling=4000, fdest=0 peer_tag=1},
callID=0x81B628F0)

!-- CCAPI invokes the Session Application
```

```
*Mar 15 22:07:11.963: cc_process_call_setup_ind (event=0x81B67E44)
handed call to app "SESSION"

*Mar 15 22:07:11.963: sess_appl: ev(23=CC_EV_CALL_SETUP_IND),
cid(88), disp(0)


The primary command to debug end-to-end VoIP calls is debug voip
ccapi inout. The output from a call debug is shown below. !-- Action:
A VoIP call is originated through the Telephony SPI (pots leg) to
!-- extension 5000.  <some output has been omitted>


maui-voip-austin#debug voip ccapi inout

voip ccAPI function enter/exit debugging is on


!-- Call leg identification, source peer: Call originated from dial-
peer 1 pots
!-- (extension 4000)


*Mar 15 22:07:11.959: cc_api_call_setup_ind (vdbPtr=0x81B09EFC,
callInfo={called=, calling=4000, fdest=0 peer_tag=1},
callID=0x81B628F0)

!-- CCAPI invokes the Session Application


*Mar 15 22:07:11.963: cc_process_call_setup_ind (event=0x81B67E44)
handed call to app "SESSION"

*Mar 15 22:07:11.963: sess_appl: ev(23=CC_EV_CALL_SETUP_IND),
cid(88), disp(0)


!-- Allocate call leg identifiers "callid = 0x59"


*Mar 15 22:07:11.963: ccCallSetContext (callID=0x58,
context=0x81BAF154)

*Mar 15 22:07:11.963: ccCallSetupAck (callID=0x58)


!-- Instruct VTSP to generate dialtone


*Mar 15 22:07:11.963: ccGenerateTone (callID=0x58 tone=8)


!-- VTSP passes digits to CCAPI


*Mar 15
22:07:20.275:cc_api_call_digit_begin(vdbPtr=0x81B09EFC,callID=0x58,di
git=5,
flags=0x1, timestamp=0xC2E63BB7, expiration=0x0)

*Mar 15 22:07:20.279: sess_appl: ev(10=CC_EV_CALL_DIGIT_BEGIN),
cid(88), disp(0)

*Mar 15 22:07:20.279: ssaTraceSct: cid(88)st(0)oldst(0)cfid(-
1)csize(0)in(1)fDest(0)

*Mar 15 22:07:20.279: ssaIgnore cid(88), st(0),oldst(0), ev(10)
```



```
*Mar 15 22:07:20.327: cc_api_call_digit (vdbPtr=0x81B09EFC,
callID=0x58, digit=5, duration=100)

*Mar 15 22:07:20.327: sess_appl: ev(9=CC_EV_CALL_DIGIT), cid(88),
disp(0)

*Mar 15 22:07:20.327: ssaTraceSct: cid(88)st(0)oldst(0)cfid(-
1)csize(0)in(1)fDest(0)

*Mar 15
22:07:21.975:cc_api_call_digit_begin(vdbPtr=0x81B09EFC,callID=0x58,di
git=0,

flags=0x1, timestamp=0xC2E63BB7, expiration=0x0)

*Mar 15 22:07:21.979: sess_appl: ev(10=CC_EV_CALL_DIGIT_BEGIN),
cid(88), disp(0)

*Mar 15 22:07:21.979: ssaTraceSct: cid(88)st(0)oldst(0)cfid(-
1)csize(0)in(1)fDest(0)

*Mar 15 22:07:21.979: ssaIgnore cid(88), st(0),oldst(0), ev(10)

*Mar 15 22:07:22.075: cc_api_call_digit (vdbPtr=0x81B09EFC,
callID=0x58, digit=0, duration=150)

*Mar 15 22:07:22.079: sess_appl: ev(9=CC_EV_CALL_DIGIT), cid(88),
disp(0)

*Mar 15 22:07:22.079: ssaTraceSct: cid(88)st(0)oldst(0)cfid(-
1)csize(0)in(1)fDest(0)

*Mar 15 22:07:23.235: cc_api_call_digit_begin (vdbPtr=0x81B09EFC,
callID=0x58, d

git=0, flags=0x1, timestamp=0xC2E63BB7, expiration=0x0)

*Mar 15 22:07:23.239: sess_appl: ev(10=CC_EV_CALL_DIGIT_BEGIN),
cid(88), disp(0)

*Mar 15 22:07:23.239: ssaTraceSct: cid(88)st(0)oldst(0)cfid(-
1)csize(0)in(1)fDes

t(0)

*Mar 15 22:07:23.239: ssaIgnore cid(88), st(0),oldst(0), ev(10)

*Mar 15 22:07:23.335: cc_api_call_digit (vdbPtr=0x81B09EFC,
callID=0x58, digit=0

, duration=150)

*Mar 15 22:07:23.339: sess_appl: ev(9=CC_EV_CALL_DIGIT), cid(88),
disp(0)

*Mar 15 22:07:23.339: ssaTraceSct: cid(88)st(0)oldst(0)cfid(-
1)csize(0)in(1)fDes

t(0)

*Mar 15 22:07:25.147: cc_api_call_digit_begin (vdbPtr=0x81B09EFC,
callID=0x58, d

igit=0, flags=0x1, timestamp=0xC2E63BB7, expiration=0x0)

*Mar 15 22:07:25.147: sess_appl: ev(10=CC_EV_CALL_DIGIT_BEGIN),
cid(88), disp(0)

*Mar 15 22:07:25.147: ssaTraceSct: cid(88)st(0)oldst(0)cfid(-
1)csize(0)in(1)fDes

t(0)

*Mar 15 22:07:25.147: ssaIgnore cid(88), st(0),oldst(0), ev(10)

*Mar 15 22:07:25.255: cc_api_call_digit (vdbPtr=0x81B09EFC,
callID=0x58, digit=0

, duration=160)
```

```
*Mar 15 22:07:25.259: sess_appl: ev(9=CC_EV_CALL_DIGIT), cid(88),
disp(0)

*Mar 15 22:07:25.259: ssaTraceSct: cid(88)st(0)oldst(0)cfid(-
1)csize(0)in(1)fDes

t(0)


!-- Matched dial-peer 2 voip. Destination number 5000


*Mar 15 22:07:25.259: ssaSetupPeer cid(88) peer list:tag(2) called
number(5000)

*Mar 15 22:07:25.259: ssaSetupPeer cid(88), destPat(5000),
matched(4), prefix(),

peer(81C04A10)


!-- Continue to call an interface and start the next call leg


*Mar 15 22:07:25.259: ccCallProceeding (callID=0x58, prog_ind=0x0)

*Mar 15 22:07:25.259: ccCallSetupRequest (Inbound call = 0x58,
outbound peer =2,

dest=, params=0x81BAF168 mode=0, *callID=0x81B6DE58)

*Mar 15 22:07:25.259: callingNumber=4000, calledNumber=5000,
redirectNumber=


!-- VoIP call setup


*Mar 15 22:07:25.263: ccIFCallSetupRequest: (vdbPtr=0x81A75558,
dest=,
callParams={called=5000, calling=4000, fdest=0, voice_peer_tag=2},
mode=0x0)

*Mar 15 22:07:25.263: ccCallSetContext (callID=0x59,
context=0x81BAF3E4)

*Mar 15 22:07:25.375: ccCallAlert (callID=0x58, prog_ind=0x8,
sig_ind=0x1)


!-- POTS and VOIP call legs are tied together


*Mar 15 22:07:25.375: ccConferenceCreate (confID=0x81B6DEA0,
callID1=0x58, callI

D2=0x59, tag=0x0)

*Mar 15 22:07:25.375: cc_api_bridge_done (confID=0x1E,
srcIF=0x81B09EFC, srcCall

ID=0x58, dstCallID=0x59, disposition=0, tag=0x0)


!-- Exchange capability bitmasks with remote VoIP gateway
!-- (Codec, VAD, VoIP or FAX, FAX-rate, etc)


*Mar 15 22:07:26.127: cc_api_caps_ind (dstVdbPtr=0x81B09EFC,
dstCallId=0x58, src
```



```
CallId=0x59,caps={codec=0x4, fax_rate=0x2, vad=0x2, modem=0x1
codec_bytes=20,
signal_type=0})


!-- Both gateways agree on capabilities

*Mar 15 22:07:26.127: cc_api_caps_ack (dstVdbPtr=0x81B09EFC,
dstCallId=0x58, src

CallId=0x59, caps={codec=0x4, fax_rate=0x2, vad=0x2, modem=0x1
codec_bytes=20,
signal_type=0})

*Mar 15 22:07:26.139: cc_api_caps_ack (dstVdbPtr=0x81A75558,
dstCallId=0x59, src

CallId=0x58, caps={codec=0x4, fax_rate=0x2, vad=0x2, modem=0x1
codec_bytes=20,
signal_type=0})

*Mar 15 22:07:35.259: cc_api_call_digit (vdbPtr=0x81B09EFC,
callID=0x58, digit=T

, duration=0)

*Mar 15 22:07:35.259: sess_appl: ev(9=CC_EV_CALL_DIGIT), cid(88),
disp(0)

*Mar 15 22:07:35.259: ssaTraceSct:
cid(88)st(4)oldst(3)cfid(30)csize(0)in(1)fDes

t(0)-cid2(89)st2(4)oldst2(1)

*Mar 15 22:07:35.399: cc_api_call_connected(vdbPtr=0x81A75558,
callID=0x59)

*Mar 15 22:07:35.399: sess_appl: ev(8=CC_EV_CALL_CONNECTED), cid(89),
disp(0)

*Mar 15 22:07:35.399: ssaTraceSct:
cid(89)st(4)oldst(1)cfid(30)csize(0)in(0)fDes

t(0)-cid2(88)st2(4)oldst2(4)


!-- VoIP call is connected


*Mar 15 22:07:35.399: ccCallConnect (callID=0x58)


!-- VoIP call is disconnected. Cause = 0x10

*Mar 15 23:29:39.530: ccCallDisconnect (callID=0x5B, cause=0x10
tag=0x0)
```


Laboratory Exercise 6-1: Voice over IP with H.323

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Instructor router with gatekeeper functionality enabled

Exercise Objective

You need to be able to call all other router-attached and PBX-attached telephones in the classroom. Since 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 exercise, you will implement a scalable Voice over IP (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 exercise, you will be able to:

- 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

Command List

The commands used in this exercise are described in the table here.

Table 1: H.323 Commands

Command	Description
debug cch323 h225	Traces the state transition of the H.225 state machine based on the processed event. This command is executed in privileged mode.
debug gatekeeper server	Traces all the message exchanges between the Cisco IOS gatekeeper and the external applications. This command is executed in privileged mode.
gatekeeper	Enables gatekeeper functionality. This command is executed in global configuration mode.
gateway	Enables gateway configuration. This command is executed in global configuration mode.
h323-gateway voip interface	Specifies that this interface's IP address will be used to register with the gatekeeper. This command is executed in interface configuration mode.
h323-gateway voip id ***gatekeeper-id*** **ipaddr** ***gatekeeper-ip-addr***	Defines the name and location of the gatekeeper for this gateway. This command is executed in interface configuration mode.
h323-gateway voip h323-id	Defines the name that will be used to identify this gateway to the gatekeeper. This command is executed in interface configuration mode.
session target ras	Specifies that the registration, admission, and status (RAS) protocol is being used to determine the IP address of the session target. This command is executed in dial-peer configuration mode.
show gatekeeper ***option***	Displays various parameters and status for a gatekeeper. This command is executed in user mode on the gatekeeper.
show gateway	Shows if the gateway is connected to the gatekeeper. This command is executed in user mode on the gateway.
zone local | remote	Statically specifies a local or remote zone. Parameters include gatekeeper name, domain name, and IP address. This command is executed in gk configuration mode.
zone prefix	Specifies which group of telephone numbers are reachable via a specific gatekeeper. The prefix typically contains wildcards for number summarization. This command is executed in gk configuration mode.

Job Aids

These job aids are available to help you complete the laboratory exercise:

- Instructor's Router Gateway is gk, IP address is 192.168.100.1

Task 1

In this task, you will configure your router to be a gateway that registers with a gatekeeper. This is a single zone configuration since all the voice-enabled routers will register to a single gatekeeper.

Exercise Procedure

Complete these steps:

Step 1 Enable **debug** in order 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 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** output to observe the interactions between your router and the gatekeeper. The following 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 command-line interface (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 it has registered the destination patterns from your plain old telephone service (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 your router's H.323-ID? _____

What zone is your gateway part of? _____

Step 4 Create a dial peer to use RAS for all calls to destinations outside your pod.

Step 5 Establish a voice call to a telephone in another pod. Use the **show call active voice** command to provide the following information:

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 following information:

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.

Exercise Verification

You have completed this exercise when you attain these results:

- Configure and verify that your gateway has registered with a gatekeeper.
- Call all other telephones in the classroom.

Task 2

In this task, you will configure your voice-enabled router to be both a gateway and a gatekeeper. Your router's gateway function will be configured to register internally with your router's gatekeeper function. Since all the other routers are also configuring themselves to be gatekeepers, this will be a multizone configuration.

Complete these steps:

Step 1 Prior to this step, you have already established VoIP dial peers to your partner's telephones. 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. 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. To enable gatekeeper functionality, perform the following tasks:

- Enable gatekeeper functionality.
- Define your local zone information. For your zone name, use "gk" + 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 your gatekeeper is not in shutdown state.
- Define all remote zones using the same naming and addressing convention as in the previous task. Do not include the other router in your pod as a remote. Configure **zone prefixes** 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 process 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.

Exercise Verification

You have completed this exercise when you attain these results:

- Configure and verify that your gateway has registered with a gatekeeper.
- Configure and verify gatekeeper functionality on your router.
- Call all other telephones in the classroom.

Laboratory Exercise 6-2: Configuring Voice over IP with SIP

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

This lab exercise will use all the equipment listed for the standard CVOICE labs. In addition, the lab will need:

- Session initiation protocol (SIP) proxy server on instructor LAN

Exercise Objective

In this exercise, you will use SIP direct (user agent to user agent) and proxy call control procedures to establish Voice over IP (VoIP) calls.

After completing this exercise, you will be able to:

- Configure dial peers to use SIP call control procedures to set up VoIP calls

Command List

The commands used in this exercise are described in the table here.

Table 1: SIP Commands

Command	Description
debug ccsip ***options***	Displays various real-time SIP call information. This command is executed in privileged mode.
session protocol sipv2	Specifies that the VoIP dial peer should use SIP/call control when processing the call. This command is executed in dial-peer configuration mode.
session target sip-server	Specifies the use of the proxy server. This command is executed in dial-peer configuration mode.
show sip-ua ***options***	Displays various parameters for SIP. This command is executed in privileged mode.
sip-server ipv4:x.x.x.x	Specifies the IP address of the SIP proxy server. This command is executed in sip-ua configuration mode.
sip-ua	Enters SIP User Agent configuration mode. This command is executed in global configuration mode.

Job Aids

These job aids are available to help you complete the laboratory exercise:

- SIP Proxy Server IP address 192.168.100.10

Task 1: Configuring for SIP

In this exercise, you will be configuring your router to initiate calls with your partner's router using SIP. In the beginning of the exercise, you will use SIP direct, user agent to user agent. After that, you will configure your router to use the proxy server.

Exercise 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's configuration.

Step 1 Modify the existing VoIP dial peers that point to your partner's telephones 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 your partner's router.

Step 2 Use the **show call active voice** command to verify that you now have SIP call legs when placing a call to your partner's telephone.

Step 3 Enable SIP debugging and place a call between your telephone and your partner's 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 Prepare to use a SIP proxy server by configuring the IP address of the Cisco SIP proxy server. The proxy server address is 192.168.100.10.

Step 6 Now that you have configured the SIP proxy server address, you no longer need to specify an IP address in the **session target** of each VoIP dial peer. Modify the **session target** in the same dial peer used in Step 1. Replace the IP address in the **session target** with **sip-server**.

Step 7 Enable SIP debugging and place a call to your partner's router-attached telephone. Observe the interactions among your router's UA client, the proxy server, and the destination router's UA server.

Step 8 Again, investigate the status of SIP with variations of the **show sip-ua** command.

Step 9 Do not save your configuration at this time. You will be asked to reload the router after the next lab.

Exercise Verification

You have completed this exercise when you attain these results:

- Establish voice calls between telephones connected to your routers by way of direct SIP call control procedures.
- Establish voice calls between telephones connected to your routers by way of SIP proxy server call control procedures.

Laboratory Exercise 6-3: Voice over IP with Media Gateway Control Protocol

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- Media Gateway Control Protocol (MGCP) call agent resident on the instructor LAN

Exercise Objective

In this exercise, you will use a call agent to establish voice calls between telephones connected to MGCP residential gateways.

After completing this exercise, you will be able to:

- 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

Command List

The commands used in this exercise are described in the table here.

Table 1: MGCP Commands

Command	Description
application mgcpapp	Enables MGCP for the voice port configured in this dial peer. This command is executed in dial-peer configuration mode.
ccm-manager mgcp	Enables support for Cisco CallManager (CCM) MGCP. This command is executed in global configuration mode.
debug ccm-manager ***options***	Displays real-time CCM MGCP information. This command is executed in privileged mode.
debug mgcp ***options***	Displays real-time MGCP call information. This command is executed in privileged mode.
mgcp	Enables MGCP functionality on the router. This command is executed in global configuration mode.
mgcp call-agent ***ip-address***	Specifies the MGCP call agent IP address. This command is executed in global configuration mode.
show call application voice summary	Displays a list of available applications. This command is executed in user mode.
show ccm-manager	Displays CCM MGCP information. This command is executed in user mode.
debug ccm-manager ***options***	Displays real-time CCM MGCP information. This command is executed in privileged mode.

Job Aids

These job aids are available to help you complete the laboratory exercise:

- MGCP call agent IP address is 192.168.100.100

Task 1: MGCP Calls

Exercise 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's 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 it.

Step 2 One of the Foreign Exchange Service (FXS) ports is already configured and in use as an intelligent endpoint. Use the other FXS port as a dumb endpoint that will use the MGCP call agent to provide the processing capabilities. This will be accomplished by configuring the dial peer that points to that port for MGCP.

Move the telephone to the unused FXS port on the voice-enabled router.

Step 3 Enable MGCP on the routers in your pod by specifying MGCP and configuring the IP address of the call agent.

Step 4 Modify the plain old telephone service (POTS) dial peers for the other FXS on your router by removing the destination pattern and entering the **application mgcpapp** command.

Step 5 Use **show** commands to verify that the gateway is registered with the CallManager.

Step 6 Enable **debug** and establish a call between the telephones connected to your routers. Analyze the **debug** output, looking for the interactions between your router and the call agent and between your router and the destination router.

Step 7 Investigate the status of MGCP with variations of the **show mgcp** command.

Step 8 Reload the router. Make sure you say no when asked if you want to save your configuration.

Exercise Verification

You have completed this exercise when you attain these results:

- Establish voice calls between the telephones connected to your routers by way of MGCP.

Laboratory Exercise 7-1: Quality of Service

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- FTP client and server software

Exercise Objective

In this exercise, you will observe the incremental and combined effects of applying Quality of Service (QoS) concepts to improve voice quality end-to-end.

After completing this exercise, you will be able to:

- Implement quality improvements on low-speed links with QoS features such as fragmentation, interleave, 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 each QoS feature contributes to overall improvements in voice quality

Command List

The commands used in this exercise are described in the table here.

Table 1: QoS Commands

Command	Description
bandwidth ***bandwidth(Kbps)***	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 ***map-class-name***	Applies the Frame Relay map class that was created previously. This command is executed in data-link connection identifier (DLCI) configuration mode.
class-map ***name***	Creates a class map and enters class map configuration mode. This command is executed in global configuration mode.
class ***name***	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.
encapsulation ppp	Enables Point-to-Point Protocol (PPP) encapsulation. Configure in both serial and multilink interfaces.
fair-queue	Enables weighted fair queuing (WFQ) on the interface. This command is executed in MP-interface configuration mode.
frame-relay bc ***value***	Specifies the committed burst value. This value should be 1/100 of the committed information rate (CIR) for a 10-ms maximum burst delay. This command is executed in map-class configuration mode.
frame-relay cir ***value***	Specifies the CIR of the Frame 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 ***fragment-size-in-bytes***	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 ***dlci-number***	Enables DLCI configuration mode for a specific DLCI. This command is executed in interface configuration mode.
frame-relay traffic-shaping	Enables Frame Relay traffic shaping on the interface. This command is executed in interface configuration mode.
interface multilink ***interface-no***	Creates an MP interface and enters multilink interface configuration mode This command is executed in global configuration mode.
ip qos dscp ***option***	Specifies the differentiated services code point for the dial peer. Use class selector 5 (cs5) to specify IP precedence of 5. This command is executed in dial-peer configuration mode.

map-class frame-relay ***name***	Creates a Frame Relay map class and enters map class configuration mode. This command is executed in global configuration mode.
match ip dscp cs5	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 ***group-no***	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 ***name***	Creates a policy map and enters policy map configuration mode. This command is executed in global configuration mode.
ppp multilink	Enables Multilink PPP (MLP) on an interface. Configure in both serial and multilink interfaces.
ppp multilink fragment delay ***delay-max***	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 a MLP bundle. This command is executed in MP-interface configuration mode.
priority ***bandwidth***	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 ***direction name***	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 ***int-number***	Displays the policy applied to the interface. This command is executed in use mode.

Job Aids

There are no job aids for this laboratory exercise.

Task 1

Exercise Procedure

Complete these steps:

Part 1 – Check voice quality

Step 1 Initially, in the classroom lab, there are no QoS parameters configured. The only QoS in place is the default queuing mechanism, which is typically WFQ. Ensure your VoIP dial peer is not pointing to your partner's Frame Relay link IP address. This ensures that the call travels across the PPP link, not the Frame Relay link. Once you have verified that you are not using the Frame Relay link IP address, shut down the Frame Relay interface. Establish a VoIP call between your routers, then start a file transfer between the client/servers in your pod. Note any degradation in the voice quality. Is the quality the same in both directions of the call? Compare comments with your partner.

Part 2 – Multilink PPP

Step 1 Write down the IP address of your PPP serial interface. _____ Remove the interface IP address. This address is reused in the multilink interface.

Step 2 Set the bandwidth to reflect the clock rate of 72,000. This is necessary for the router to calculate the correct fragment sizes.

Step 3 Create a multilink interface, configuring it with the IP address from Part 2, Step 1, MLP, WFQ, fragmentation, and interleave. Assign the same multilink group number under both the serial interface and the multilink interface to link them together.

Step 4 Coordinate with your partner to start testing when both sides of the PPP link are configured. Start a file transfer between the client/servers in your pod and compare the voice quality while transferring data with the voice quality while not transferring data. Is there a difference in quality? Is the quality the same in both directions? Discuss the results with your partner.

Part 3 – Frame Relay

Step 1 Shut down the PPP interface. Re-enable your Frame Relay interface and ensure that you have connectivity to your partner's router across the frame cloud.

Step 2 Test voice and file transfers together. Because only the Frame Relay connection is active, the voice call and the file transfer are dependent on a Frame Relay permanent virtual circuit (PVC). Comment on the voice quality. Is the quality the same in both directions? Discuss the quality with your partner.

Step 3 Implement Frame Relay traffic shaping and fragmentation according to the recommendations discussed during the lecture. The recommendation for this lab is to use 64-kbps CIR and to configure for 10-ms delay for committed burst and for fragmentation. If you cannot ping the other router after implementing traffic shaping, verify that you have traffic shaping turned on, that WFQ is enabled, and that there is a fragment size set. Verify that you have applied the map class to the appropriate DLCI pointing to your partner's router. Ensure the map class name you apply at the DLCI matches exactly with the name of the map class you defined. The names are case sensitive.

Step 4 Once again, repeat the combined voice and file transfer test and note any changes in voice quality. Has the quality improved since enabling of traffic shaping? Remember that at this point, voice is not getting priority over data. Data is simply getting fragmented so that voice does not have to wait as long to get to the output queue.

Step 5 Re-enable your PPP interface. Test connectivity across PPP by pinging your partner's PPP interface address.

Part 4 – Prioritization

Step 1 Modify the appropriate dial peers to add an IP precedence of five to all VoIP packets. Retest and note voice quality issues. Watch what happens to the download speed when speech is present on the call and when speech is absent from the call.

Step 2 Enable Low Latency Queuing (LLQ) on the low-speed serial interfaces and retest combined voice and data. Note any quality issues. There are three basic parts to configuring LLQ. First, identify which traffic gets priority, using a class map. Second, specify what the special treatment is, using the policy map. Third, configure an interface to use the defined policy using the service policy statement.

Step 3 To enable LLQ complete the following tasks:

1. Create a class map for the VoIP traffic and define match criteria. Since you configured the VoIP dial peers to an IP differentiated services code point (DSCP) code of cs5, use that as the match criteria.

2. Create a policy map and associate to the VoIP class map. Specify that voice traffic identified in the previously created class map should go to the priority queue with enough bandwidth for one call.

3. Apply the policy map to the outbound WAN interfaces. For the PPP link, apply it to the multilink interface. For the Frame Relay link, apply it to the Frame Relay map class. To do this, you must remove WFQ. Apply the policy outbound on the interface. For the Frame Relay link, apply it to the Frame Relay map class. Use **show** commands to view the new policy and see that it is applied to the multilink interface.

4. Retest the combined voice and data and note any quality issues.

Part 5 – Benefits of Fragmentation and Interleave

Step 1 Confirm that fragmentation and interleave (implemented earlier) are having a beneficial effect by changing the fragment size on the PPP and Frame Relay links to 1500 bytes. Changing the fragment size in Frame Relay is straightforward. What command do you use to change the fragment size in PPP?

_____

Step 2 To how many milliseconds do you set the PPP setting? _____

Step 3 Repeat the combined voice and data tests and note any changes in the voice quality. Again, watch the download and see what happens to the data transfer.

Step 4 Restore the 10-ms fragmentation configurations on both your PPP and Frame Relay links.

Part 6 – End-to-End QoS

During the remainder of this lab, you investigate end-to-end quality of service by creating calls using more than one data link at a time. Changes are made only on the R1 router, so for this step, work together to enable the configuration and test the calls. Your instructor identifies the pairing of the pods.

Step 1 Shut down the Frame Relay interface on the R1 router of the pod. Ensure that you can reach the client/server in the adjacent pod from the client/server connected to your R1 router. Perform a trace from your R1 client/server to the partner's R1 server to show that you are traversing different data links. The trace should show the path going across the PPP link to R2, then across the Frame Relay link to the other pod's R2, then across their PPP link to the other pod's R1.

Step 2 Establish a voice call from the telephone on your R1 router to the telephone on the other pod's R1 router. Pay attention to the voice quality.

Step 3 Start a file transfer between client/servers in the partnering pods while the voice call is still established. Again, pay attention to the voice quality in both directions during the file transfer. Watch the speed of the file transfer.

Step 4 Save your configuration.

Exercise Verification

You have completed this exercise when you attain these results:

- Maintain voice quality while transferring data over a shared path.

Laboratory Exercise 7-2: Call Admission Control

Complete the laboratory exercise to practice what you have learned in this lesson.

Required Resources

These are the resources and equipment required to complete this exercise:

- No new resources are required.

Exercise Objective

In this exercise, you will implement Call Admission Control (CAC) by limiting the maximum number of connections on dial peers. You will then implement CAC by using Resource Reservation Protocol (RSVP). Next, you will implement CAC using an H.323 gatekeeper. Throughout the lab exercise, you will use **show** and **debug** commands to verify CAC.

After completing this exercise, you will be able to:

- Implement CAC by setting the dial-peer maximum connections
- Implement CAC with RSVP
- Implement CAC with an H.323 gatekeeper
- Confirm that CAC techniques can effectively limit the number of Voice over IP (VoIP) calls

Command List

The commands used in this exercise are described in the table here.

Table 1: Call Admission Control Commands

Command	Description
acc-qos ***best-effort*** | ***controlled-load*** | ***guaranteed-delay***	Specifies the acceptable quality of service (QoS) for any inbound or outbound call on a VoIP dial peer. This command is executed in dial-peer mode.
bandwidth interzone {**default** | **zone** ***zone-name***} ***bandwidth-size***	Specifies the maximum aggregate bandwidth for H.323 traffic. This command is executed in gatekeeper mode.
call rsvp-sync	Enables synchronization between RSVP signaling and the voice signaling protocol. This command is on by default. This command is executed in global config mode.
ip rsvp bandwidth ***interface-kbps single-flow-kbps***	Enables RSVP for IP on an interface and specifies bandwidth limits. This command is executed in interface mode.
max-conn	Specifies the maximum number of allowed connections to and from the plain old telephone service (POTS) dial peer. The valid range is 1-2147483647. This command is executed in dial-peer mode.
req-qos ***best-effort*** | ***controlled-load*** | ***guaranteed-delay***	Specifies the desired QoS to be used in reaching a specified dial peer. This command is executed in dial-peer mode.

Job Aids

These job aids are available to help you complete the laboratory exercises:

- None

Task 1: Dial Peer Call Admission Control

In this task, you will configure CAC to limit the number of calls over the PPP link between your routers.

Exercise Procedure

Complete these steps:

Step 1 Shut down the Frame Relay interface in your router. You will use only the PPP connection for this task.

Step 2 Verify that you can establish two voice calls over the PPP link in your pod. Ensure that the dial peer uses the PPP link and that the same dial peer is used for both calls.

Step 3 Limit the calls allowed for this dial peer to one. Verify that only one call is allowed. Observe the call control message on your router console if you attempt to make more than the maximum number of calls allowed.

Step 4 Provide an alternate path for excess calls if possible. Limiting calls is a way to ensure that bandwidth is not oversubscribed. The second call is allowed by using the Public Switched Telephone Network (PSTN) as an alternate path. Create a dial peer to reroute excess calls to the PSTN. Use appropriate **show** commands to verify that the excess call is being properly rerouted while the first call uses the PPP link. Remove the command entered in Step 3 and re-enable the Frame Relay interface to prepare for the next task.

Exercise Verification

You have completed this exercise when you attain these results:

- Limit the number of calls on a dial peer.
- Reroute excess calls via the PSTN.
- Verify that excess calls are rerouted.

Task 2: RSVP Call Admission Control

In this task, you will implement CAC using RSVP.

Exercise Procedure

Complete these steps:

Step 1 Remove the Low Latency Queuing (LLQ) configuration from the previous lab.

Step 2 Configure RSVP on the PPP and Frame Relay interfaces to synchronize with the voice signaling protocol. Configure the requested and accepted QoS to be guaranteed delay. Configure RSVP on both routers and applicable dial peers in your pod.

Step 3 Configure the Frame Relay interface to allow only one call. Configure the PPP interface to allow only one call. Be sure to allow enough bandwidth for each type of interface.

Step 4 Confirm that two calls can be completed between your routers simultaneously. One call will use the Frame Relay path; the other call will use the PPP path.

Step 5 Confirm that RSVP is making a reservation using the appropriate **show** and **debug** commands. How much bandwidth does RSVP reserve for each call? _____

Step 6 Start a file transfer between your partner and you. Place a call to your partner's telephone. Is the voice quality acceptable?

Step 7 Watch the implementation of RSVP with appropriate **show** commands.

Step 8 Disable RSVP by removing the RSVP commands from the dial peers and interfaces to prepare for the next task.

Exercise Verification

You have completed this exercise when you attain these results:

- Implement call admission control with RSVP.
- Verify implementation of RSVP with **show** commands.

Task 3: H.323 Call Admission Control

In this task, you will implement CAC using gatekeepers.

Exercise Procedure

Complete these steps:

Step 1 Configure all H.323 Gatekeepers to permit only one call between the local zone and any other zone.

Step 2 Attempt to make two calls to an adjacent pod (zone). One call should go through, the other should produce a busy signal.

Step 3 Watch the progress of your first and second calls with appropriate **show** and **debug** commands.

Exercise Verification

You have completed this exercise when you attain these results:

- Limit the number of interzone calls on a gatekeeper.
- Verify CAC on a gatekeeper.

A

Answer Key

This document presents the correct answers and solutions for the course practices, assessments, and lab exercises.

Outline

This resource includes these sections:

- Practice Items

Practice Items

The practice items and solutions are listed here. The shaded answer options are the correct answers. This is a presentation of all course practice items.

Module 1: Introduction to Packet Voice Technologies

Lesson: Traditional Telephony

Q1) Match the component of a telephony network with the function it performs.

A) Edge device

B) Local loop

C) Private or CO switch

D) Trunk

_____ 1. handles signaling, call routing, call setup and call teardown **(C)**

_____ 2. provides a path between two switches **(D)**

_____ 3. connects to the PSTN **(A)**

_____ 4. interfaces to the telephone company network **(B)**

Q2) Which type of trunk connects two local telephone company COs?

A) tie trunk

B) CO trunk

C) interoffice trunk

D) all of the above

Q3) Two CO switch components that make a telephone work include a battery, ring generator, dial tone generator, _____, and _____. (Choose two.)

A) tandem switch

B) current detector

C) terminal interface

D) control complex

E) digit register

Q4) Dial tone is generated when the _____.

A) user dials a number

B) flow of current is interrupted

C) DTMF tones are detected

D) dial register is ready

Q5) The difference between a PBX and a key system is that a _____.

A) key system handles more calls

B) key system is digital only

C) key system is not a switch

D) key system is analog only

Q6) Which three of the following are components of a key system? (Choose three.)

A) terminal interface

B) key service unit

C) telephones

D) control complex

E) switching network

F) system software

Q7) Match the type of signaling to its description.

A) supervisory signaling

B) informational signaling

C) address signaling

_____ 1. is a type of signaling that uses either pulse or DTMF **(C)**

_____ 2. provides call progress indicators to the initiator of a call **(B)**

_____ 3. is a type of signaling that monitors on-hook/off-hook transitions and provides call notification **(A)**

Q8) CAS passes signaling _____.

A) in the same channel as voice for T1

B) in the D channel

C) using frequency-division multiplexing

D) using DTMF frequencies

Q9) Which multiplexing process is used by TDM?

A) Timeslots are assigned to different channels, regardless of whether there is data to transmit.

B) Timeslots are assigned to different channels depending on which traffic has a higher priority at that time.

C) All timeslots are used by the channel that is transmitting data at that time.

D) Timeslots are assigned to the channel that starts transmitting first, and are used by the other channels as they become available.

Q10) DSL is an example of _____.

A) frequency-division multiplexing

B) phase-division multiplexing

C) time-division multiplexing

D) statistical time-division multiplexing

Lesson: Packetized Telephony Networks

Q1) Which of the following is NOT a benefit of packet voice networks?

A) consolidated voice and data network expenses

B) guaranteed delivery of digital voice

C) greater innovation in services

D) more efficient use of bandwidth and equipment

Q2) What is the main drawback of migrating to packet technology?

A) Upgrade cost may override potential cost savings.

B) New devices may not be compatible with the existing PBX.

C) Unified communications may overload the network.

D) Voice transmission cost may increase.

Q3) Which function is NOT performed by call control?

A) establishing a call

B) maintaining a call

C) routing a call

D) disconnecting a call

Q4) Which two functions are performed by the call setup component of call control? (Choose two.)

A) monitors the quality of the connection

B) determines the destination of the call

C) tracks packet count and packet loss

D) notifies voice-enabled devices to make resources available for next call

E) sends the call initiator a busy signal if sufficient bandwidth is not available

Q5) Which two protocols are examples of distributed call control ? (Choose two.)

A) MGCP

B) H.323

C) SIP

D) Megaco

Q6) In the centralized call control model, signaling is performed by the _____.

A) gateway

B) gatekeeper

C) MCU

D) call agent

Q7) The three purposes of a gatekeeper is to provide _____. (Choose three.)

A) CAC call admission control

B) access to the PSTN

C) bandwidth control and management

D) billing and accounting

E) address translation

Q8) Match the component of a packet voice network to its function.

A) gateway

B) MCU

C) IP Pphone

D) call agent

E) application server

F) videoconference station

_____ 1. translates between the IP network and the PSTN **(A)**

_____ 2. provides access for end user participation in videoconferencing **(F)**

_____ 3. brings IP voice to the desktop **(C)**

_____ 4. provides real-time connectivity for videoconferencing **(B)**

_____ 5. provides services such as voice mail and unified messaging **(E)**

_____ 6. performs call control on behalf of IP Pphones **(D)**

Q9) Two guarantees of real-time traffic include _____. (Choose two.)

A) delay

B) routing

C) decibels

D) timing

Q10) Traditional data networks were designed for _____.

A) real-time packet transmission

B) guaranteed delivery

C) guaranteed timing

D) best-effort packet delivery

Lesson: IP Telephony Applications

Q1) In E & M signaling, “E” refers to the _____.

A) electromagnet

B) ring

C) electrical ground

D) tip

E) Erlang

Q2) The FXS interface provides a direct connection to the _____.

A) CO

B) E & M trunk

C) telephone

D) gatekeeper

Q3) An E1 interface can carry up to _____ conversations simultaneously.

A) 16

B) 24

C) 30

D) 32

Q4) What type of signaling is used when a T1 interface uses CCS?

A) robbed-bit signaling

B) Megaco

C) Q.931

D) H.323

Q5) What kind of cable is used to connect an IP Phone to the network?

A) RJ-11

B) wireless transceiver

C) serial crossover

D) RJ-41

E) RJ-45

Q6) How many queues does each port on a Cisco IP Phone contain?

A) 2

B) 3

C) 4

D) 12

Q7) In a campus LAN environment, the multipoint control unit provides _____.

A) central call-processing capabilities

B) configuration capabilities

C) conferencing capabilities

D) extended-calling capabilities

E) call-pickup capabilities

Q8) Which two of the following key issues must be considered when designing the campus infrastructure for voice? (Choose two.)

A) ability to power IP Phones

B) processing power of the gatekeeper

C) size of DRAM in the routers

D) ease of IP addressing

Q9) Which two models are used for designing enterprise networks? (Choose two.)

A) service provider

B) carrier class

C) distributed

D) centralized

E) remote site

Q10) What is the function of the SRTS component of a centralized voice enterprise network?

A) connects IP Phones on remote sites to Cisco CallManager

B) provides local call-processing capabilities in case of a WAN outage

C) configures routing plans for the gateways

D) serves as the primary voice path between sites

Q11) To be competitive, service providers must provide their business customers with _____ alternatives to the PSTN for voice and data services.

A) more extensive, less complicated

B) more exhaustive, less limited

C) more digital, less analog

D) more efficient, less expensive

Q12) In service provider environments, the network design must accommodate _____.

A) support for TDM

B) automated configuration of IP networks

C) support for SIP, H.323, and MGCP

D) a full Class A IP-address block

Module 2: Analog and Digital Voice Connections

Lesson: Analog Voice Basics

Q1) In most local-loop connections, what does the ring wire tie to?

A) battery

B) ground

C) telephone

D) switch

Q2) What allows the current to flow around the loop?

A) when the ring wire connects to the negative side of a power source

B) when the tip wire connects to the ground

C) when the telephone goes off hook

D) when the telephone goes on hook

Q3) What are the three different types of local-loop signaling? (Choose three.)

A) address signaling

B) coding signaling

C) control signaling

D) informational signaling

E) remote signaling

F) supervisory signaling

Q4) What two tools do subscriber and telephone companies use to notify each other of call status? (Choose two.)

A) audible tones

B) digital signatures

C) electrical current

D) pulse packets

E) tagged packets

Q5) What happens when the switch hook is in a closed state?

A) only the ringer is active

B) the telephone is on hook

C) the current flows through the electrical loop

D) the current cannot flow through the electrical loop This is the correct answer

Q6) What is the ringing tone in the United States?

A) one 2-second tone followed by 2 seconds of silence

B) one 2-second tone followed by 4 seconds of silence

C) two 0.4-second rings separated by 0.2 seconds of silence, followed by 2 seconds of silence

D) two 2-second rings separated by 4 seconds of silence

Q7) In the United States, what is the required ratio of the break/make cycle for rotary-dial phones?

A) 60-percent break to 40-percent make

B) 60-percent make to 40-percent break

C) 80-percent break to 20-percent make

D) 80-percent make to 20-percent break

Q8) On a DTMF phone, each button on the keypad is associated with _____.

A) a series of pulses

B) a set of dial tones

C) a make and break cycle

D) a set of high and low frequencies

Q9) Which call progress indicator is used to let you know that the telephone company is working on completing the call?

A) busy

B) confirmation tone

C) dial tone

D) ring-back

Q10) Which tone is used to indicate that all the local telephone circuits are busy?

A) busy

B) ringback

C) all circuits busy

D) reorder

Q11) Match the trunk type with its description.

A) private trunk lines

B) CO trunks

C) interoffice trunks

D) FX trunks

_____ 1. trunk interfaces that connect to station equipment or office equipment **(D)**

_____ 2. trunk circuit that connects two local telephone company COs **(C)**

_____ 3. direct connection between a PBX and the local CO **(B)**

_____ 4. dedicated circuits that connect PBXs **(A)**

Q12) What type of trunk is required on a home telephone?

A) private tie-line

B) CO trunk

C) interoffice trunk

D) FX trunk

Q13) Which statement describes the problem of glare in loop-start signaling?

A) The trunk is simultaneously seized from both ends.

B) The signal is so loud that it cannot be understood.

C) The trunk is overloaded with too many messages.

D) The ring voltage is so high that it interferes with communication.

Q14) Which trunk signaling method uses separate wires for voice and signaling?

A) loop-start

B) ground-start

C) E&M

D) CAS

Q15) Which E&M signaling type is not supported by Cisco voice equipment?

A) Type I

B) Type II

C) Type III

D) Type IV

E) Type V

Q16) Which type of E&M signaling is useful when the PBX and the Cisco equipment are in different buildings on the campus?

A) Type I

B) Type II

C) Type III

D) Type IV

E) Type V

Q17) Which type of E&M signaling is used when all the equipment is mechanical?

A) Wink Start

B) immediate start

C) delay start

Q18) Which type of E&M signaling is the most commonly used?

A) Wink Start

B) immediate start

C) delay start

Q19) How much echo delay is generally not problematic?

A) below 50 ms

B) below 100 ms

C) below 120 ms

D) below 150 ms

Q20) Which two factors contribute to echo problems? (Choose two.)

A) attenuation

B) crosstalk

C) delay

D) electric current on the line

E) incorrect voltage

F) loudness

Q21) Which method is used to reduce echo on Cisco devices?

A) echo suppression

B) echo cancellation

C) echo correction

D) echo return loss

Q22) In what situations is it problematic to use echo suppression?

A) for voice transmission

B) for half-duplex modem connections

C) for full-duplex modem connections

D) all of the above

Lesson: Analog to Digital Voice Encoding

Q1) Which of these steps is optional in analog to digital conversion?

A) compression

B) encoding

C) quantization

D) sampling

Q2) How often is the analog to digital signal conversion sampling process repeated for telephone voice channel service?

A) 8000 times per call

B) 8000 times per voice sample

C) 8000 times per second

D) 8000 times per minute

Q3) What device is used to reconstruct the digital signal to its original analog signal?

A) modem

B) compander

C) filter

D) codec

Q4) During the process of converting digital signals back to analog signals, each received 8-bit word is decoded to recover _____.

A) the PAM signal

B) the number that defines the amplitude of the sample

C) the analog wave form

D) the base10 number that corresponds to the 8-bit number

Q5) What frequency range is the telephone channel designed for?

A) 20 to 20,000 Hz

B) 200 to 9000 Hz

C) 300 to 3400 Hz

D) 4000 to 8000 Hz

Q6) If voice is sampled at a rate of one sample every 125 microseconds, what is the highest frequency of sound in the channel according to the Nyquist Theorem?

A) 3400 Hz

B) 4000 Hz

C) 8000 Hz

D) 20,000 Hz

Q7) What is the problem with linear sampling of analog signals?

A) Small-amplitude signals have a higher noise-to-signal ratio.

B) The signal cannot be sampled instantaneously at the transmitter.

C) The sampling interval is too long for high-amplitude signals.

D) The samples do not contain enough information for accurate conversion.

Q8) Which quantization method is used in the United States?

A) α-law

B) μ-law

C) PCM

D) Nyquist

Q9) Which coding schemes are examples of waveform algorithms?

A) PCM

B) ADPCM

C) CELP

D) LDCELP

E) CS-ACELP

Q10) Which is NOT a function of waveform algorithms?

A) sample analog signals at 8000 times per second

B) use predictive differential method to reduce bandwidth

C) use codebooks to match stored waveshapes in the receiver codebook

D) do not take advantage of speech characteristics

Q11) What are the two differences between G.729 and G.729A compression? (Choose two.)

A) the platforms that support them

B) complexity

C) compression delay

D) standards body

E) demands on the processor

Q12) Which two G.729 codec provides built-in IETF VAD and CNG? (Choose two.)

A) G.729

B) G.729A

C) G.729B

D) G.729AB

E) all of the above

F) none of the above

Q13) Which compression technique is used with G.711 codecs?

A) ADPCM

B) CS-ACELP

C) LDCELP

D) PCM

Q14) Which compression standard has the lowest bandwidth requirement?

A) ADPCM

B) CS-ACELP

C) LDCELP

D) PCM

Q15) What is the level of distortion for a MOS rating of 4?

A) imperceptible

B) just perceptible but not annoying

C) perceptible and slightly annoying

D) annoying but not objectionable

Q16) What is the rating scale for measuring voice quality with PSQM?

A) 1 to 5 where 1 is worst

B) 1 to 5 where 5 is worst

C) 0 to 6.5 where 0 is worst

D) 0 to 6.5 where 6.5 is worst

Lesson: Signaling Systems

Q1) In a T1 using CAS, what is the F bit in the ESF for?

A) framing

B) CRC

C) supervisory channel

D) all of the above

Q2) In CAS, what type of control information is provided by the A and B bits in SF?

A) near- and far-end off-hook

B) idle

C) busy

D) ringing

E) addressing

F) all of the above

Q3) How many timeslots are there in an E1 frame using CAS?

A) 16

B) 24

C) 30

D) 32

Q4) In an E1 frame using CAS, which bits are reserved for signaling?

A) all the bits in time slot 16

B) all the bits in time slot 17

C) the first bit in time slot 17

D) the least significant bit in time slot 1

Q5) Which signaling method is NOT an example of CCS?

A) DPNSS

B) ISDN

C) QSIG

D) RBS

E) SS7

Q6) If vendors use a proprietary CCS protocol between their PBXs, what must Cisco devices be configured for?

A) CCS

B) CCSS7

C) SS7

D) T-CCS

Q7) What type of information is carried in the D channel of ISDN?

A) voice

B) video

C) data

D) signaling

Q8) How many B channels and signal channels are implemented on a PRI T1?

A) 1 B channel and 1 signaling channel

B) 2 B channels and 1 signaling channel

C) 23 B channels and 1 signaling channel

D) 30 B channels and 1 signaling channel

Q9) What type of interfaces support QSIG?

A) BRI

B) PRI

C) T1

D) E1

Q10) Which ISDN standard is QSIG based on?

A) Q.2931

B) Q.931

C) Q.920

D) Q.93B

Q11) Which function is performed by SS7?

A) call establishment

B) billing

C) routing

D) information exchange

E) all of the above

Q12) SS7 was developed by _____.

A) IETF

B) ISO

C) ITU

D) Cisco

Q13) Why is signal conversion necessary?

A) To allow different systems to signal each other

B) To convert G.711 to G.729

C) To convert voice to data

D) To encode and compress voice

Q14) Which signaling method would be required between a CO and an ISDN switch?

A) loop start

B) T1 CAS

C) SS7

D) E1 CAS

E) RBS

Lesson: Fax and Modem over Voice over IP

Q1) Which device acts as a fax modem in Cisco fax relay?

A) the DSP

B) the gateway

C) the modem

D) the gatekeeper

Q2) What speed does the fax modem operate at in Cisco fax relay?

A) 64 kbps

B) 52 kbps

C) 16 kbps

D) 9.6 kbps

Q3) Which Cisco device or application can be configured as a T.38 gateway?

A) Cisco IP Phone

B) Cisco call-processing agents

C) Cisco carrier-class call agents

D) Cisco voice-enabled routers

Q4) What is the advantage of using T.38 as compared to Cisco proprietary fax relay?

A) T.38 has a faster transmission rate.

B) T.38 allows delivery of documents to virtual fax machines.

C) T.38 uses a more efficient transmission methodology.

D) all of the above.

Q5) How can you provide temporary storage in a packet network for fax messages that need to be delivered ?

A) Configure a fax relay buffer on the on-ramp gateways.

B) Configure T.37 store-and-forward fax relay on the on-ramp gateways.

C) Configure T.37 store-and-forward fax relay on the off-ramp gateways.

D) Configure T.37 store-and-forward fax relay on both the on-ramp and off-ramp gateways.

Q6) In T.37 store-and-forward fax relay, which parameters must be configured to instruct the SMTP server to notify e-mail originators of the status of their messages?

A) DSN parameters

B) fax parameters

C) MDN parameters

D) MTA parameters

Q7) Which call control protocol does NOT support fax passthrough?

A) H.323

B) SIP

C) MGCP

D) SGCP

Q8) Which feature is enabled for fax passthrough using Cisco IOS Release 12.0(3)T and later?

A) echo cancellation

B) echo suppression

C) VAD

D) PCM

Q9) What is the advantage of using modem relay as compared to modem passthrough?

A) Modem relay requires less bandwidth.

B) Modem relay is supported by more call control protocols.

C) Modem relay provides more interoperability.

D) Modem relay uses compression mechanisms.

Q10) Which protocol is used to carry modem signals across the network using Modem Relay?

A) SMTP

B) SPRT

C) MGCP

D) RTP

Q11) How does modem passthrough differ from fax passthrough?

A) VAD is enabled.

B) G.711 is not used.

C) There is a computer modem at each end.

D) 64-kbps bandwidth is required.

Q12) How can you reduce the effects of packet loss in modem passthrough?

A) by introducing packet redundancy

B) by increasing bandwidth

C) by reducing latency

D) by using dedicated lines

Module 3: Configuring Voice Interfaces

Lesson: Voice Port Configuration

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 **(C)**

_____ 2. a type of call that is handled entirely by one router and does not go across an external network **(A)**

_____ 3. a type of call that is rerouted through a secondary path when the primary path fails **(D)**

_____ 4. a type of call that may be routed through one or more routers, but stays on the same network **(B)**

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 if you wanted to set the dial tone, the busy tone, and the ringback tone?

A) cptone

B) ring frequency

C) ring cadence

D) description

E) signal

Q4) Which situations would probably require you to change the FXS port default settings?

A) when the caller and the called party are in different parts of the country

B) when the caller and the called party are in different countries

C) when the connection is a trunk to a PBX

D) when the configuration of the FXS port matches the configuration of the local PSTN switch

Q5) Which statement 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 that is overseen by the network administrator

Q6) Which configuration parameter would you need to set for a device that does not support DTMF dialing?

A) signal

B) dial type

C) description

D) supervisory disconnect

Q7) What might happen if the wrong cable scheme is specified during E&M port configuration?

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) In which type of signaling does the router provide current on the E-lead immediately upon seeing current on the M lead?

A) Delay-Start signaling

B) Immediate-Start signaling

C) Wink-Start signaling

D) Q signaling

Q9) Which parameter do you need to configure if you want to set the number of seconds the system should wait for the subsequent digit to be dialed after the caller has input the initial digit?

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) The configuration commands required for ISDN voice functionality include **isdn switch-type**, **isdn incoming-voice voice**, **qsig signaling**, and _____.

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) When you are configuring T-CSS in a VoIP network, the **trunk** *number* must match the number entered in the _____ 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) none of the above

Q18) Which two conditions can you check 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.

E) The signaling type matches the signaling type configured on the PBX.

Lesson: Adjusting Voice Quality

Q1) Which factor can cause echo during transmission of voice over an IP network?

A) incorrect input levels

B) incorrect output levels

C) impedance mismatch

D) all of the above

Q2) Analog voice routers operate best when the receive level from an analog source is set at _____.

A) –2 dB

B) –3 dB

C) –9 dB

D) –14 dB

Q3) Which two parameters 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

Q4) What 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

Q5) Which command is used to suppress listener echo?

A) echo-cancel enable

B) echo-cancel coverage

C) non-linear

D) **no** echo-cancel enable

Q6) Which of these commands is enabled by default?

A) echo-cancel enable

B) echo-cancel coverage

C) non-linear

D) no echo-cancel enable

Module 4: Voice Dial Peers

Lesson: Call Establishment Principles

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 and one outbound dial peer

D) all four dial peers

Q3) Arrange the steps in the call setup process in the correct order. Below is the correct order:

Step 1 The POTS call arrives at Router 1 and an inbound POTS dial peer is matched.

Step 2 Router 1 creates an inbound POTS call leg and assigns it a Call ID.

Step 3 Router 1 uses the dialed string to match an outbound Voice-Network dial peer.

Step 4 Router 1 creates an outbound Voice-Network call leg and assigns it a Call ID.

Step 5 The Voice-Network call request arrives at Router 2 and an inbound Voice-Network dial peer is matched.

Step 6 Router 2 creates the inbound Voice-Network call leg and assigns it a Call ID.

Step 7 At this point, both Router 1 and Router 2 negotiate Voice Network capabilities and applications, if required.

Step 8 Router 2 uses the dialed string to match an outbound POTS dial peer.

Step 9 Router 2 creates an outbound POTS call leg, assigns it a Call ID.

Q4) What is the role of the terminating router if the originating router requests non-default voice capabilities?

A) It negotiates with the originating router until the default capabilities are accepted.

B) It reconfigures the ports to meet the requested capabilities.

C) It matches an inbound voice network dial peer that has the requested capabilities.

D) It terminates the call.

Lesson: Dial Peers

Q1) 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

Q2) The address is configured on each dial peer and is called a _____.

A) telephone number

B) number range

C) destination pattern

D) call endpoint

Q3) Which two parameters need to 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

Q4) 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

Q5) 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

Q6) What happens if a loopback address is 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) None of the above.

Q7) 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.

Q8) Which special character in a destination pattern string is used as a wildcard?

A) asterisk (*)

B) pound sign (#)

C) comma (,)

D) period (.)

E) brackets ([])

Q9) 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) None of the above.

Q10) What is the default dial-peer configuration for inbound POTS peers?

A) any codec

B) no ivr application

C) vad enabled

D) no rsvp support

E) ip precedence 0

Q11) Which configurable parameter is set only for POTS dial peers?

A) answer-address

B) destination-pattern

C) incoming called-number

D) port

Q12) In what order does the router attempt to match the called number of the call setup request with a dial-peer attribute? Correct answer:

incoming called-number

answer-address

destination-pattern

port

Q13) Write the number of the dial peer configuration in the space beside the specified destination to which it is matched first.

1. dial-peer voice 1 pots
   destination-pattern .T
   port 1/0:1

2. dial-peer voice 2 pots
   destination-pattern 555[0-2,5]…
   port 1/1/0

3. dial-peer voice 1 pots
   destination-pattern 5553…
   port 1/0:1

4. dial-peer voice 1 pots
   destination-pattern 5553216
   port 1/0.1

___**1**___ A) dialed number is 5551234

___**2**___ B) dialed number is 5550000

___**1**___ C) dialed number is 567-1234

___**4**___ D) dialed number is 5553216

___**3**___ E) dialed number is 5553000

___**1**___ F) dialed number is 555000

Q14) When the router is matching 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*

Q15) 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 **(C)**

_____ 2. sets priority for dial peers **(A)**

_____ 3. stops dial-peer hunting on the dial peer **(D)**

_____ 4. changes the default selection order for hunting through dial peers **(B)**

Q16) 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
```

Q17) By default, which 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.

Q18) 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

Q19) The user is dialing the number 5551234. In the space below each dial peer configuration, specify what digits are passed out of the telephony interface.

A)
```
dial-peer voice 1 pots
destination-pattern 5551234
port 1/0/0
```

_____**None**_____

B)
```
dial-peer voice 2 pots
destination-pattern 555…
port 1/0/0
```

_____**123**_____

C)
```
dial-peer voice 3 voip
destination-pattern 555….
session target ipv4: 10.0.0.1
```

_____**5551234**_____

D)
```
dial-peer voice 4 pots
destination-pattern 555….
port 1/0/0
no digit-strip
```

_____**5551234**_____

E)
```
dial-peer voice 5 pots
destination-pattern 555….
port 1/0/0
forward-digits 6
```

_____**555123**_____

Q20) What is the default behavior of a terminating router when it is matching a dial string to an outbound POTS dial peer?

A) The router removes the left-most digits that match the destination pattern, and forwards the remaining digits.

B) The router strips off the wildcard digits and forwards only the matching digits

C) The router forwards all the digits without attempting a match.

D) The router does not forward any digits if it cannot match them.

Q21) A **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

Q22) When 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: Special-Purpose Connections

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** parameter 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

E) all of the above

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's 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.

Module 5 Introduction to Voice over IP

Lesson: Requirements of Voice in an IP Internetwork

Q1) What is one cause of jitter when voice packets are transmitted over an IP network?

A) congestion leading to instantaneous buffer utilization

B) the corruptive effect of noise

C) the loss of some voice packets on high-traffic lines

D) use of the PSTN

Q2) How can you ensure proper delivery of voice packets over an IP network?

A) by using QoS parameters

B) by using Frame Relay as the Layer-2 technology

C) by using circuit-switched paths only

D) by using high-speed links

Q3) According to ITU G.114, what is the maximum delay that VoIP can tolerate before voice quality starts to degrade?

A) 120 ms

B) 150 ms

C) 200 ms

D) 250 ms

Q4) What conditions can result in voice packets being dropped during transmission across an IP network? (Choose two.)

A) The network quality is poor.

B) There is too much variable delay in the network.

C) The router is down.

D) The switch handles data packets only.

Q5) Match the Cisco IOS tools for enhanced voice throughput with their description.

A) queuing

B) congestion avoidance

C) header compression

D) RSVP

E) fragmentation

_____ 1. provides preferential treatment for priority traffic **(B)**

_____ 2. holds packets so that they can be handled with a specific priority when they leave the router interface **(A)**

_____ 3. defines the maximum size of a data packet **(E)**

_____ 4. enables the network to provide differentiated levels of service to specific flows of data **(D)**

_____ 5. saves bandwidth by compressing the header **(C)**

Q6) Which technique is used to prevent excessive serialization delay?

A) queuing

B) congestion avoidance

C) header compression

D) RSVP

E) fragmentation

Q7) Which protocol automatically reorders packets?

A) TDM

B) IP

C) UDP

D) RTP

Q8) What is the function of RTCP in ensuring consistent delivery of voice packets in an IP network?

A) reorders the voice packets through the use of sequence numbers

B) retimes the voice packets based on time stamps

C) sends occasional report packets for delivery monitoring

D) all of the above

Q9) Which Cisco technology can be used to provide proactive network management?

A) Cisco IOS services

B) Cisco AVVID

C) Cisco CallManager

D) CiscoWorks 2000

Q10) What do traditional telephony networks typically use to provide redundancy?

A) multiple servers

B) multilayer switches

C) multiple connections between switches

D) all of the above

Lesson: Voice over IP vs. Voice over Frame Relay or Voice over ATM

Q1) What is the advantage of VoATM and VoFR networks?

A) Data units arrive in sequence.

B) Network failures are difficult to recover from.

C) Network failures are automatically routed around.

D) Data arrives out of sequence.

Q2) What is the advantage of IP networks?

A) Data units arrive in sequence.

B) Network failures are difficult to recover from.

C) Network failures are automatically routed around.

D) Data arrives out of sequence.

Q3) Which field does TCP/IP use to mark packets as high priority?

A) FRF.11

B) payload

C) CRC

D) HL

E) ToS

Q4) In VoFR and VoATM networks, what does the FRF.11 header in voice packets identify? (Choose two.)

A) destination address

B) payload type

C) subchannels

D) protocol

E) version

Q5) What does the presence of the payload length field in FRF.11 encapsulation indicate?

A) the contents of the payload

B) the presence of two or more subframes in the payload field

C) the presence of the payload type and CID MSB fields

D) the most significant bits of subchannel ID

Q6) What is the default payload size for G.729 codecs using VoFR?

A) 10 bytes

B) 20 bytes

C) 30 bytes

D) 40 bytes

Q7) Which attribute of a voice packet can be configured to change the bandwidth requirements?

A) overhead

B) payload size

C) FRF.11 header

D) CRC

Q8) What would be the required bandwidth for a packet with an 80-byte payload and an 8-byte overhead if a codec with 8000 bps bandwidth is used?

A) 801 bps

B) 8000 bps

C) 8800 bps

D) 64000 bps

Q9) What is the default payload for a G.729 codec used with VoATM?

A) 30 bytes

B) 45 bytes

C) 48 bytes

D) 240 bytes

Q10) What is the size of the payload in an ATM cell?

A) 30 bytes

B) 45 bytes

C) 48 bytes

D) variable

Q11) What is the length of the AAL5 trailer in an ATM cell?

A) 3 bytes

B) 5 bytes

C) 8 bytes

D) variable

Q12) What would be the required bandwidth for a VoATM call if the payload size is 50 bytes and a G.729 codec is used?

A) 15000 bps

B) 24000 bps

C) 25000 bps

D) 85000 bps

Lesson: Gateways and Their Roles

Q1) Which type of devices can be used as a voice gateway? (Choose two.)

A) telephone

B) codec

C) modem

D) switch

E) router

Q2) The gateway translates the digitized signal or voice into the appropriate analog or digital signal to be sent to the PSTN based on _____.

A) the configuration of the gateway

B) the protocols being used on the network

C) the default settings of the gateway

D) the information inside the voice packet

Q3) Why is it important to know which country the gateway will be located in when you are planning a network? (Choose two.)

A) You need to know the network requirements.

B) You need to know the standards for PSTN connections.

C) You need to know the design requirements.

D) You need to know the functions required of the gateway.

E) You need to know any legal issues involving encryption services.

Q4) Which signaling protocol can be used with gateways?

A) H.323

B) MGCP

C) SIP

D) all of the above

Q5) Issues that need to be addressed at the central site include dial plan integration, voice mail integration, gateway for PBX interconnect, and _____.

A) signaling interconnection type

B) carrier-class performance

C) scalability

D) in-line power requirements for IP phones

Q6) 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, in-line power, and security features are to be implemented.

C) It affects zone configurations.

D) It determines the Cisco IOS version that should be used.

Q7) Which feature of the service provider network benefits from redundant interconnect capabilities directly into the PSTN?

A) SS7 interconnections

B) carrier-class performance

C) scalability

D) all of the above

Q8) Which feature of a service provider gateway, if implemented properly, can provide carrier-class performance?

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: Encapsulating Voice in IP Packets

Q1) Match the VoIP protocol with its function.

A) H.323

B) MGCP

C) SIP

D) RTP

E) RTCP

_____ 1. adopts a modified form of the URL addressing scheme used within e-mail based on SMTP **(C)**

_____ 2. allows control of VoIP gateways connected to external call control devices **(B)**

_____ 3. reports statistics on the call **(E)**

_____ 4. defines all aspects of synchronized voice, video, and data transmission **(A)**

_____ 5. provides sequence numbers and timestamps for orderly processing of voice packets **(D)**

Q2) Which VoIP protocol operates at the transport layer of the OSI model?

A) H.323

B) MGCP

C) SIP

D) RTP

Q3) Which type of session is RTP primarily designed for?

A) unicast

B) multicast

C) broadcast

D) all of the above

Q4) Which Layer-4 protocol is used for transporting RTCP packets?

A) IP

B) TCP

C) UDP

D) RTP

Q5) What is the size of the IP/UDP/RTP header?

A) 20 bytes

B) 32 bytes

C) 40 bytes

D) 48 bytes

Q6) To what size does CRTP compress the IP/UDP/RTP header when UDP checksums are used?

A) 2 bytes

B) 4 bytes

C) 8 bytes

D) 12 bytes

Q7) Which conditions necessitate the use of CRTP? (Choose two.)

A) need for bandwidth conservation on WAN interfaces

B) high-speed interfaces

C) links that are as slow as 4 Mbps

D) narrowband links

E) broadband links

Q8) Where should compression be enabled?

A) on each link that requires it

B) on the entire network

C) on both sides of a slow link

D) on links with high traffic

E) on all links using RTP

Lesson: Bandwidth Requirements

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 it uses.

A) G.711

B) G.726

C) G.728

D) G.729

E) G.723

_____ 1. ADPCM **(B)**

_____ 2. CS-ACELP **(D)**

_____ 3. LD-CELP **(C)**

_____ 4. MPMLQ **(E)**

_____ 5. PCM **(A)**

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 would be the size of voice samples from Cisco voice equipment if a G.728 codec were used?

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) Which factor lowers bandwidth requirements for a VoIP call?

A) larger sample size

B) more bandwidth required by the codec

C) more overhead associated with the data link

D) none of the above

Q8) 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) 11600 bps

C) 17200 bps

D) 19200 bps

Q9) What is the function of comfort noise generation?

A) provides features such as music on hold

B) provides white noise to make the call appear normally connected to both parties

C) provides full voice call bandwidth

D) reduces the delay in VoIP connections

Q10) If the bandwidth requirement for a voice call over Frame Relay is 11395 bps, what would be the bandwidth requirement if VAD was used?

A) 3989 bps

B) 7407 bps

C) 9116 bps

D) 11180 bps

Lesson: Security Implications

Q1) 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) all of the above

Q2) In which situation can the firewall inspect the packet for call setup?

A) when the firewall is configured for call setup

B) when the VPN terminates outside the firewall

C) when the VPN terminates inside the firewall

D) when the firewall does not recognize the signal or payload ports

Q3) 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

Q4) 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) all of the above

Q5) How does hardware encryption reduce overhead and delay as compared to software encryption?

A) It optimizes the encryption algorithm and data path.

B) It handles all processing in a dedicated encryption processor.

C) It does not rely on CPU resources.

D) It uses proper QoS technologies.

Q6) Which type of encryption technology may not be used on international networks because of government restrictions?

A) DES

B) 3DES

C) ESP

D) IPSec

Q7) How many bytes of overhead does VPN add to the voice packet?

A) 20 bytes

B) 40 bytes

C) 20 to 60 bytes

D) 40 to 80 bytes

Q8) Which type of VPN is most commonly used today?

A) IPSec

B) ESP

C) PPTP

D) L2TP

Module 6: VoIP Signaling and Call Control

Lesson: Need for Signaling and Call Control

Q1) What are two examples of signaling systems used in traditional telephony? (Choose two.)

A) red-light signaling

B) YBTM Signaling

C) Common Channel Signaling System 7

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) Which protocol is NOT an example of a Voice over IP call control model?

A) SIP

B) RSVP

C) Megaco

D) SAP

Q4) Match the call control model with its description.

A) H.323

B) MGCP

C) H.248

D) RTSP

E) Skinny

_____ 1. describes a model for controlled, on-demand delivery of real-time audio and video **(D)**

_____ 2. allows control of VoIP gateways from a call agent **(B)**

_____ **3.** controls communication between the gateway's subcomponents **(C)**

_____ 4. provides basic call processing, signaling, and connection services to configured devices **(E)**

_____ 5. describes the architecture to support multimedia communications over networks without QoS guarantees **(A)**

Q5) On a VoIP network, which protocol carries the audio path?

A) RTP

B) SIP

C) H.323

D) MGCP

Q6) Which call control function is required at the gateway to allow two endpoints using different call control models to communicate?

A) authentication

B) compression

C) registration

D) translation

Q7) Which of the following 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 information does each endpoint need to recognize in order to create RTP sessions?

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) call detail records

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) Call detail records

_____ 1. ensures resources are being used effectively **(C)**

_____ 2. allows determination of call distribution and grade of service **(D)**

_____ 3. supports users with services such as address resolution **(B)**

_____ 4. monitors call activity in real time **(A)**

Q11) Which benefits are associated with call detail records? (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 call detail records

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 it can reach?

A) a list of all the telephone numbers it can reach

B) a list of all the IP addresses it can reach

C) a routing table

D) a prefix

Q15) What are two aspects of admission control? (Choose two.)

A) authentication

B) authorization

C) call detail record creation

D) bandwidth management

E) address resolution

Q16) What information do the bandwidth management and call admission control functions use to monitor bandwidth consumption?

A) router configuration

B) network speed

C) call detail records

D) call status data

Q17) Which device has the most intelligence in a centralized call control model?

A) originating endpoint

B) central controller

C) gateway

D) gatekeeper

E) intermediate router

Q18) Which statements regarding endpoints are true in a centralized call control model?

A) Endpoints automatically provide dial tone when a telephone goes off hook.

B) Endpoints automatically start call setup when a telephone goes off hook.

C) Endpoints manage calls that are in progress.

D) Endpoints provide physical connections for the telephone network.

E) Endpoints decide when and how to use their interconnect abilities.

Q19) Which capability of a distributed call control model endpoint is the same as a centralized call control endpoint?

A) Endpoints manage the telephone interface.

B) Endpoints autonomously initiate call setup.

C) Endpoints route calls in case a common control component fails.

D) Endpoints have a media path between them.

Q20) What may be one reason for endpoints to share common control components in a distributed call control model?

A) bandwidth conservation

B) scalability

C) ease of call setup

D) faster routing

Q21) What are the advantages of a distributed call control model? (Choose two.)

A) It provides superior configuration control.

B) It provides fault tolerance.

C) It simplifies introduction of new features.

D) It simplifies deployment of additional endpoints.

E) It provides superior maintenance of the endpoint database.

Q22) What are the advantages of a centralized call control model? (Choose two.)

A) It minimizes dependence on network resources.

B) It provides superior maintenance of the dial plan.

C) It simplifies introduction of supplementary services.

D) It simplifies deployment of additional endpoints.

E) It reduces bandwidth consumption.

Lesson: H.323

Q1) Which tasks are performed by the RAS signaling function of H.225? (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 **(A)**

_____ 2. requests a change in capability of the media stream **(D)**

_____ 3. negotiates audio, video, and codec capability between the endpoints **(B)**

_____ 4. is used to resolve conflicts during the call **(C)**

Q3) Which H.323 component can be collocated 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

F) none of the above

Q7) Put in the correct order the steps involved in H.323 basic call setup without a gatekeeper.

Step 1 The originating gateway initiates an H.225.0 session with the destination gateway on registered TCP port 1720.

Step 2 The gateway determines the IP address of the destination gateway internally.

Step 3 Call setup procedures based on Q.931 create a call signaling channel between the endpoints.

Step 4 The endpoints open another channel for the H.245 control function.

Step 5 The H.245 control function negotiates capabilities and exchanges logical channel descriptions.

Step 6 The logical channel descriptions open RTP sessions.

Step 7 The endpoints exchange multimedia over the RTP sessions.

Q8) How does the abbreviated call-setup procedure in version 2 of 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) It establishes an H.245 control channel with both endpoints.

B) It performs call setup, call function, and call control functions.

C) It represents the other endpoint for call signaling only.

D) It passes on the originating endpoint's request 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 admission request from the originating endpoint

C) the call setup request from the gateway

D) network statistics

Q11) 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

Q12) 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

Q13) Which 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

Q14) In a call flow with multiple gatekeepers, which gatekeeper allows the remote endpoint to accept the incoming call?

A) the gatekeeper that the originating endpoint is associated with

B) the gatekeeper that the remote endpoint is associated with

C) the gatekeeper that first received the admission request

D) the gatekeeper that is available to set up the call

Q15) In H.323, which survivability strategy allows two gatekeepers to share an IP address?

A) HSRP

B) multiple gateways configured for the same prefix

C) multiple gatekeepers configured for the same prefix

D) multiple gatekeepers with gatekeeper discovery

Q16) 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.

Q17) What is the role of an H.323 proxy server?

A) provides an alternate path when the direct path is not be the most appropriate path

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

Q18) 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

Q19) Which Cisco application supports H.323 gatekeepers?

A) Cisco IP Phone

B) Cisco CallManager

C) Cisco Secure Integrated Software

D) Cisco voice-enabled switches

Q20) Which H.323 component is supported by Cisco SC2200 signaling controllers?

A) terminals

B) gateways

C) gatekeepers

D) MCU

Q21) 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

Q22) When you are configuring an H.323 gateway, what 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

Q23) Which command tells the gatekeepers to define addresses locally?

A) zone prefix

B) zone local

C) zone remote

D) zone default

Q24) 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

Q25) Which **show** command is used to list the registered endpoints with ID and supported prefixes?

A) show gatekeeper gw-type-prefix

B) show gatekeeper zone prefix

C) show gatekeeper endpoints

D) show gatekeeper status

Q26) Which **debug** command should you use to monitor the activity of the H.225 and H.245 call signaling channels on a busy network? Please refer to Module 6, Lesson 2, slide Monitoring and Troubleshooting, slide notes.

A) debug h225 asn1

B) debug h225 events

C) debug h245 asn1

D) debug h245 events

E) none of the above

Lesson: SIP

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) Which of the following is NOT a SIP server?

A) registrar

B) gateway

C) redirect

D) location

E) proxy

Q4) Which SIP server is often collocated with the location server?

A) proxy

B) redirect

C) registrar

D) gateway

Q5) Which SIP method 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) 1*xx*—Informational

B) 2*xx*—Successful

C) 3*xx*—Redirection

D) 4*xx*—Client error

E) 5*xx*—Server error

F) 6*xx*—Global failure

Q7) How does a SIP UA resolve an address?

A) It uses a local host table.

B) It uses rwhois.

C) It lets the network server resolve it.

D) All of the above.

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 needs to 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 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) Which SIP component is supported by Cisco voice-enabled AS5*xx*0 servers?

A) SIP user agent

B) SIP proxy server

C) SIP redirect server

D) SIP dial peer

Q14) Which operating environments can Cisco SIP proxy server be used with?

A) Linux (Redhat 8.0 or later)

B) Windows NT

C) Solaris 2.8

D) MacOS

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 so 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: MGCP

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) to handle the translation of video between the SCN and the packet-switched network

B) to handle the translation of audio between the SCN and the packet-switched network

C) to control the operation of the endpoints and the call agent

D) to allow only authenticated traffic into the network

Q5) According to RFC 2705, which type of MGCP endpoint represents an access 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) How many call agents can an MGCP gateway interact with?

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 **(B)**

_____ 2. supports digital circuit endpoints subject to ISDN signaling **(A)**

_____ 3. supports endpoints connected to traditional analog interfaces **(D)**

_____ 4. supports analog and digital endpoints connected to a PBX **(C)**

Q9) Why does the MGCP require the gateway to observe and report events?

A) so that it can recognize each endpoint that it supports

B) so that it can tell the endpoint what type of signal to send to the attached telephone equipment

C) so that it can recognize the signaling characteristics of each physical interface attached to the gateway

D) so that it can recognize the signaling characteristics of each logical interface attached to the gateway

Q10) What information does the MGC 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) What 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) What 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) end point

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) Which examples represent MGCP events? (Choose two.)

A) busy tone

B) continuity test

C) distinctive ringing

D) fax tones

E) hook flash

F) ringing

Q16) Which examples represent MGCP signals? (Choose two.)

A) confirm tone

B) continuity detection

C) continuity test

D) DTMF digits

E) on-hook transition

Q17) Which packages are associated with the NAS? (Choose two.)

A) multifrequency

B) DTMF

C) trunk

D) line

E) announcement server

F) RTP

Q18) Which packages are associated with the residential gateway? (Choose three.)

A) generic media

B) multifrequency

C) DTMF

D) trunk

E) network access server

F) line

Q19) A gateway that is using a digit map notifies the call agent when _____. (Choose two.)

A) each digit is collected

B) all the digits have been collected

C) the gateway finds a match for the digits

D) the digits that match the area code have been collected

E) the gateway concludes that the dialed digits cannot be matched

Q20) In the United States, how would the digit map identify digits for the local PSTN?

A) xxxx

B) 91xxxxxxxxxx

C) 9 + 7 or 10 digits

D) 9011 + upto 15 digits

Q21) Match the MGCP control command with its function.

A) EndpointConfiguration

B) NotificationRequest

C) ModifyConnection

D) AuditEndpoint

E) RestartInProgress

_____ 1. requests the status of an endpoint **(D)**

_____ 2. instructs the gateway on what action to take upon the occurrence of an event **(B)**

_____ 3. identifies the coding characteristics of the endpoint interface on the line side of the gateway **(A)**

_____ 4. notifies the call agent that the gateway and its endpoints are removed from service **(E)**

_____ 5. instructs the gateway to update its connection parameters for a previously established connection **(C)**

Q22) Which two commands are issued by a gateway? (Choose two.)

A) EndpointConfiguration

B) NotificationRequest

C) CreateConnection

D) DeleteConnection

E) RestartInProgress

Q23) Which two types of information are included in the notify (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

Q24) 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

Q25) 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.

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 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.

Q26) 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) BTS 10200 Softswitch

Q27) 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) BTS 10200 Softswitch

Q28) 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 Gateway

D) BTS 10200 Softswitch

Q29) 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

Q30) 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.

Q31) 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

Q32) 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: Comparing Call Control Models

Q1) Which call control model uses encoding that 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. Each call control model can be used more than once.

A) client

B) terminal

C) gateway

D) media gateway

_____ 1.H.323 **(C or B)**

_____ 2. SIP **(A)**

_____ 3. MGCP **(D)**

Q3) Which call control model most closely resembles the PSTN?

A) H.323

B) SGCP

C) SIP

D) MGCP

Q4) Which call control model is popular in large enterprises because of its maturity and stability?

A) H.323

B) SGCP

C) SIP

D) MGCP

Module 7: Improving and Maintaining Voice Quality

Lesson: Voice Quality Measurement

Q1) Which two factors contribute to delay variation in voice transmission? (Choose two.)

A) congestion on the network

B) electrical impedance mismatches

C) compression of packets

D) inconsistency in bandwidth

E) varying routes of packets

Q2) Which two factors affect voice clarity? (Choose two.)

A) fidelity

B) echo

C) sidetone

D) background noise

E) distance

Q3) Which 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

Q4) What is the disadvantage of using VAD on a call?

A) The cost of the call may increase.

B) The listener may hear unwanted noise.

C) The bandwidth requirement may increase.

D) The speaker may think that the connection is broken.

Q5) Which voice quality scoring system is based on subjective evaluation?

A) MOS

B) PCM

C) PSQM

D) YBTM

Q6) Why is it important to establish a baseline when using MOS for evaluating voice quality?

A) The results are linear.

B) The results are relative.

C) The results are compiled infrequently.

D) The results are too hard to interpret.

Q7) How is PSQM measured?

A) by comparing original speech with transmitted speech

B) by having listeners score transmitted speech

C) by having listeners score prerecorded sentences

D) by using Cisco equipment and software for measuring transmitted speech

Q8) What is the accuracy of PSQM as compared to other listening tests?

A) over 50 percent

B) over 65 percent

C) over 90 percent

D) over 99.9 percent

Q9) Which codec scores highest in MOS testing?

A) G.711

B) G.723.1

C) G.726

D) G.728

E) G.729

Q10) According to MOS tests, which network condition distorts voice the least?

A) 5 percent bit error rate

B) 5 percent frame error rate

C) two tandem codings

D) three tandem codings

E) low input level

Lesson: VoIP Challenges

Q1) Which feature of an IP network causes delay and delay variation in voice traffic?

A) connectionless transmission

B) fragmentation and reassembly

C) FIFO queuing

D) no error correction or acknowledgements

Q2) Which Layer 4 protocol is used for transmitting packets in VoIP networks?

A) IP

B) TCP

C) UDP

D) Frame Relay

Q3) How can you reduce jitter in a VoIP network?

A) by using de-jitter buffers

B) by using FIFO queuing

C) by using header compression

D) by using guaranteed delay

Q4) Variable delay is also known as _____.

A) non-deterministic

B) jitter

C) playout delay

D) FIFO

Q5) According to ITU-T Recommendation G.114 for national telecom administrations, how much delay is acceptable for most user applications?

A) 0 to 150 ms

B) 200 to 250 ms

C) 150 to 400 ms

D) above 400 ms

Q6) According to Cisco, what is the acceptable level of one-way delay for private networks?

A) 0 to 150 ms

B) 200 to 250 ms

C) 150 to 400 ms

D) above 400 ms

Q7) 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

Q8) Which conditions can result in voice packets being dropped?

A) slow links

B) too much noise

C) too much jitter

D) none of the above

Q9) What is the major cause of delay when voice and data packets are placed in the same output queue?

A) large packets

B) low bandwidth

C) firewalls

D) retransmission of lost packets

Q10) What two techniques can be used on slower links in a voice and data network to reduce delay in voice transmission? (Choose two.)

A) FIFO queuing

B) buffering of voice packets

C) fragmentation of large packets

D) prioritization of voice packets

E) compression of packets

Q11) What is the size of the RTP header?

A) 3 bytes

B) 5 bytes

C) 12 bytes

D) 40 bytes

Q12) Which RTP header field is used to allow multiplexing of multiple streams of data?

A) contributing source count

B) marker

C) payload type

D) sequence

E) time stamp

F) synchronization source

G) contributing source

Q13) What is one of the main benefits of using Cisco AVVID for voice and data networks?

A) seamless scalability of infrastructure and applications

B) ability to provide equal quality for voice and data

C) low cost of implementation

D) integration with legacy networks

Q14) Which factor is a prerequisite for voice networking?

A) TCP sessions

B) FIFO queuing

C) high availability

D) low cost

Lesson: Quality of Service and Good Design

Q1) Which two factors have a minimal effect on data transmissions but negatively impact voice transmissions? (Choose two.)

A) high bandwidth

B) T-1 links

C) packet loss

D) jitter

E) Layer 2 protocol

Q2) What are the two requirements of effective voice transmission over an IP network? (Choose two.)

A) low latency

B) G.711 codecs

C) reliable delivery of packets

D) use of compression algorithms

E) high-speed links

Q3) 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

Q4) 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

Q5) Which two Cisco IOS 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

Q6) 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

Q7) If you want to learn about troubleshooting QoS features provided by Cisco IOS Release 12.1(5)T, which certification course should you take?

A) Deploying Cisco QoS for Enterprise Networks

B) Implementing Cisco Quality of Service

C) Cisco IOS 12.0 Quality of Service

D) Cisco IP Telephony Network Design

Q8) Which Cisco course describes the Integrated Services and the Differentiated Services QoS models?

A) Service Level Management

B) Cisco IP Telephony Network Design

C) Deploying Cisco QoS for Enterprise Networks

D) Implementing Cisco Quality of Service

Q9) Which three areas of the Cisco.com website contain information about QoS? (Choose three.)

A) documentation

B) private

C) products

D) public

E) publications

F) support

Q10) In which area of Cisco.com would you find the document "Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)"?

A) public

B) support

C) documentation

Q11) Which title is a Cisco Press Publication that may be helpful for understanding QoS implementation?

A) Cisco IP Telephony Solution Guide

B) Designing a Long Distance VoIP Network

C) Cisco IOS 12.0 Quality of Service

D) Graphical Navigation Guide for VoIP Issues

Q12) Which title is published by Cisco Press to help network administrators understand and implement QoS?

A) Cisco IP Telephony Network Design Guide

B) IP Telephony Readiness Assessment

C) Voice over IP Fundamentals

D) Voice Quality (Quality of Service)

Q13) Which practice indicates a bad network design?

A) completely redesigning the network

B) using low latency queuing

C) ignoring Layer 3 QoS requirements

D) ignoring bandwidth requirements

Q14) 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

Q15) Which resource on Cisco.com provides information on the specific components and design methods recommended by Cisco for long-distance VoIP networks?

A) Cisco IP Telephony Network Design Guide

B) IP Telephony Readiness Assessment

C) Voice over IP Fundamentals

D) Deploying Cisco QoS for Enterprise Networks

E) Designing a Long Distance Telephone Network

Q16) Which resource on Cisco.com is meant to help organizations plan for and implement QoS?

A) Implementing Cisco Quality of Service

B) Cisco IP Telephony Network Design Guides

C) Service Level Management: Best Practices White Paper

D) Designing a Long Distance Telephone Network

E) Deploying Cisco QoS for Enterprise Networks

Lesson: Understanding Jitter

Q1) Which device buffers voice packets that arrive with variable delay and plays them out in a steady stream?

A) codec

B) DSP

C) modem

D) playout delay buffer

Q2) Which Cisco IOS service is used to synthesize packets to replace lost packets?

A) DSP

B) IVR

C) PLC

D) switch

Q3) Which device maximizes the number of correctly delivered packets and minimizes the amount of delay?

A) codec

B) DSP

C) FXS interface

D) switch

Q4) What may cause gaps in speech on a link that is using a jitter buffer?

A) an empty buffer

B) a full buffer

C) an improperly configured buffer

D) all of the above

Q5) How should you adjust the **playout-delay** parameters for fixed mode if there are gaps in speech?

A) increase the nominal delay

B) increase the minimum playout delay

C) increase the maximum playout delay

D) increase both the minimum and maximum playout delay

Q6) What change should you make to the **playout-delay** configuration if you have excessive jitter at the transmission end?

A) reduce the maximum playout delay

B) increase the minimum playout delay

C) select fixed mode

D) select adaptive mode

Q7) What happens to packets that arrive at the router later than the playout delay setting?

A) They are buffered and sent out in a steady stream.

B) The information in the packets is discarded.

C) They are placed at the head of the egress queue to reduce delay.

D) The packets are revitalized.

Q8) Which command can be used to determine the size of jitter problems?

A) show jitter

B) show call jitter

C) show call active voice

D) show active voice call

Q9) Which command is used to enable the codecs to dynamically adjust the value of the average delay depending on network conditions?

A) playout-delay mode adaptive

B) playout-delay mode adjust

C) playout-delay mode auto

D) playout-delay mode dynamic

Q10) What information do the DSP algorithms use to determine the amount of delay the jitter buffer applies to a packet?

A) average expected delay after the frame is available for playout

B) statistics from the **show** command used to determine jitter problems

C) sequence number field in the RTP packet

D) timestamps in the RTP headers of a sample of packets

Q11) In fixed mode, what does the nominal delay value signify?

A) the minimum amount of delay configurable for each voice packet

B) the amount of delay applied by the jitter buffer to each packet

C) the amount of playout delay applied by the jitter buffer at the beginning of a call

D) the minimum amount of delay applied by the jitter buffer for the duration of the call

Q12) In which mode can you specify the nominal delay value?

A) auto mode

B) adaptive mode

C) fixed mode

D) adaptive and fixed mode

Lesson: Understanding Delay

Q1) What is the purpose of a delay budget?

A) to synchronize voice traffic

B) to provide guaranteed delay for voice packets

C) to ensure that voice traffic does not exceed accepted limits for delay

D) to provide QoS services

Q2) What is the delay budget for a network?

A) the sum of fixed and variable delay from end to end for each direction

B) the sum of the one-way fixed and variable delay

C) the sum of the round-trip fixed and variable delay calculated between each device

D) the sum of the fixed and variable delay between the egress and ingress router in both directions

Q3) According to ITU-T Recommendation G.114, what is the acceptable delay for national telecom administrations?

A) 0 to 150 ms

B) 0 to 400 ms

C) 150 to 400 ms

D) above 400 ms

Q4) According to ITU-T Recommendation G.114, what is the acceptable delay for private networks?

A) 0 to 150 ms

B) 0 to 400 ms

C) 150 to 400 ms

D) above 400 ms

Q5) Match the factor that contributes to delay with its description.

A) Coder delay

B) Packetization delay

C) Serialization delay

D) Dejitter buffer delay

_____ 1. time taken to fill a packet payload with encoded speech **(B)**

_____ 2. time required to clock a frame onto the network interface **(C)**

_____ 3. time taken by the DSP to compress a block of PCM samples **(A)**

_____ 4. time a sample is held before being played out **(D)**

Q6) Which factor contributes most to variable delay on the network?

A) dejitter buffer delay

B) serialization delay

C) packetization delay

D) queuing delay

Q7) What will be the coder delay if a G.726 is loaded with four channels?

A) 2.5 ms

B) 5 ms

C) 10 ms

D) 20 ms

Q8) What is the decompression time for each sample block of voice traffic?

A) roughly twice the compression time for each block

B) roughly 3 times the compression time for each block

C) roughly 3 percent of the compression time for each block

D) roughly 10 percent of the compression time for each block

Q9) How much serialization delay is recommended by Cisco?

A) 0.2 ms

B) 0.5 ms

C) 10 ms

D) 20 ms

Q10) Identify two ways to reduce serialization delay? (Choose two.)

A) by increasing packet compression

B) by reducing the processing delay

C) by increasing the link speed

D) by prioritizing the packets

E) by decreasing the packet size

F) by reducing the queuing delay

Q11) What factors should you consider when setting the fragment size in the **frame-relay fragment** command?

A) The payload size is between 16 and 1600 bytes.

B) The serialization delay is not more than 10 ms.

C) The largest data packet is not larger than the voice packets.

D) All of the above.

Q12) Which type of delay directly affects queuing delay?

A) coder delay

B) network delay

C) serialization delay

D) packetization delay

E) dejitter buffer delay

Q13) Which two factors contribute to fixed delay only? (Choose two.)

A) coder delay

B) network delay

C) queuing delay

D) packetization delay

Q14) Which ITU-T Recommendation is considered to be a measure of acceptable end-to-end delay?

A) G.114

B) G.115

C) G.711

D) G.411

Lesson: Applying Quality of Service in the Campus

Q1) Which ports connect to access switches and core switches?

A) access ports

B) core ports

C) distribution ports

D) fast ports

Q2) What is the result of voice packet loss?

A) clipping and skips

B) echo

C) jitter

D) overlap

Q3) Which QoS service is best for high-speed campus networks?

A) fair queuing

B) queue scheduling

C) separation of queues

D) marking control and management traffic

Q4) Before you enable multiple queues on Catalyst switches, you must make sure that _____ is disabled.

A) flow control

B) signaling

C) priority queuing

D) streaming

Q5) Which type of queue scheduling provides QoS by assigning bandwidth to higher priority applications?

A) priority queue

B) interleaving

C) round robin

D) weighted round-robin

Q6) Which queue scheduling method is best suited for branch office and wiring closet switches?

A) interleaving

B) round robin

C) weighted round-robin

D) priority queue

Q7) What is used to mark control and management traffic on Catalyst 3500 and 4000 switches that are enabled for Layers 3 and 4?

A) transmission control protocols

B) access control lists

C) signaling protocols

D) firewalls

Q8) What network problems adversely affect signaling traffic for gateways and phones?

A) echo

B) congestion

C) delay and loss

D) network speed

Q9) Which strategy can you use to allow a large number of phones on a network that does not have enough IP addresses?

A) disabling routing on the network

B) configuring stub areas

C) using Class C addressing only

D) isolating the phones on an auxiliary VLAN

Q10) Which category of QoS is not suited for a campus network?

A) separation of queues

B) link efficiency

C) queue scheduling

D) marking control and management traffic

Q11) What is the recommended configuration for the receive interface in switch-wide queuing?

A) 2Q1T

B) 802.1p CoS

C) One standard FIFO queue

D) Multiple receive and transmit queues with thresholds

Q12) What type of configuration can be used for queuing with Catalyst 6000 switches?

A) 2Q1T

B) 802.1p CoS

C) One standard FIFO queue

D) Multiple receive and transmit queues with thresholds

Q13) Which command can be used to enable a second queue on the Catalyst 4000 series switches?

A) set qos

B) set qos queue 2

C) set qos map

D) set qos 0-1

Q14) Which command is used to enable switch-wide queuing?

A) set qos enable

B) enable set qos

C) qos set enable

D) qos enable set

Lesson: Applying Quality of Service in the WAN

Q1) Which characteristic describes voice traffic?

A) bursty

B) real-time

C) delay-tolerant

D) all of the above

Q2) Which requirement of voice adds significant overhead to the voice packets?

A) prioritization of voice packets

B) fragmenting the packets

C) numbering the packets

D) reducing the delay variation

Q3) Which QoS mechanisms are commonly used on the WAN? (Choose two.)

A) bandwidth provisioning

B) queue scheduling

C) traffic shaping

D) separation of queues

E) marking of control and management traffic

Q4) Which OSI layer technology affects the type of QoS measures used in the WAN?

A) Layer 1

B) Layer 2

C) Layer 3

D) Layer 4

Q5) How much of the total available bandwidth should be consumed by minimum bandwidth requirements?

A) no more than 100 percent of the bandwidth

B) no more than 99 percent of the bandwidth

C) no more than 80 percent of the bandwidth

D) no more than 75 percent of the bandwidth

Q6) Which two types of traffic are not included in the minimum bandwidth requirement calculation? (Choose two.)

A) voice media streams

B) video streams

C) HTTP traffic

D) H.323 traffic

E) overhead traffic

Q7) In optimized queuing, what kind of queuing is used for voice control signaling protocols?

A) DSCP

B) FIFO

C) WFQ

D) CBWFQ

Q8) How many traffic classes does Low Latency Queuing allow for?

A) 32

B) 48

C) 56

D) 64

Q9) Describe two ways that DiffServ improves link efficiency in a WAN? (Choose two.)

A) by specifying how the device should forward the packet

B) by providing a finer granularity of priority setting for the applications

C) by providing a finer granularity of priority setting for the devices

D) by specifying the range of acceptable link speeds

Q10) What is the size of the COS field that is used for IP precedence in an IP packet header?

A) 3 bits

B) 4 bits

C) 7 bits

D) 8 bits

Q11) When should you use QoS techniques that provide LFI?

A) when the speed of the link is less than 56 kbps

B) when the speed of the link is less than 768 kbps

C) when the speed of the link is greater than 786 kbps

D) when the speed of the link is less than 1544 kbps

Q12) Which techniques are used for providing LFI on Frame Relay links?

A) MLP

B) MLP over ATM

C) FRF.12

D) G.711

E) G.729

Q13) Which type of links is traffic shaping NOT suitable for?

A) ATM links

B) Frame Relay links

C) Ethernet

D) links with variable access speeds

Q14) On what type of links can traffic shaping mechanisms be used to limit jitter?

A) Frame Relay links

B) ATM links

C) point-to-point links

D) all of the above

Q15) Which statement describes CAC as a QoS technique?

A) specifies bandwidth for a link

B) frees up bandwidth for higher priority traffic

C) reroutes calls that exceed the specified bandwidth

D) all of the above

Q16) Which Cisco application can be used to implement CAC on an entire network?

A) Cisco IOS

B) Cisco CallManager

C) CiscoWorks 2000

D) IVR

Q17) Describe two ways that FRF.12 identifies fragmented frames? (Choose two.)

A) by adding an extended header to the frame

B) by including a 1-byte flag in the header

C) by fragmenting the packets into fixed-size frames

D) by adding sequence numbers to the frames

E) by sending FRF.12 signaling to the destination

Q18) If FRTS is enabled on a link, what happens to voice frames when the network becomes congested?

A) Frames that exceed specified bandwidth are rerouted over another link, such as a PSTN.

B) Frames that exceed specified bandwidth are buffered and transmitted when congestion is reduced.

C) Frames that exceed specified bandwidth are marked DE and dropped.

D) Frames that exceed specified bandwidth are fragmented and given sequence numbers.

Q19) What is the size of a typical G.729 voice packet?

A) 20 bytes

B) 66 bytes

C) 214 bytes

D) 1500 bytes

Q20) How does LFI reduce delay and jitter for voice traffic in a WAN?

A) It queues high-priority voice traffic ahead of data traffic.

B) It fragments large voice packets and interleaves data packets among the fragments.

C) It fragments large data packets and interleaves voice packets among the fragments.

D) It reroutes voice traffic over faster connections.

Q21) What is the purpose of a policy map?

A) defines the voice signaling and traffic class maps

B) defines how the link resources are assigned to the map classes

C) assigns a queue for voice signaling traffic

D) defines how to classify traffic that does not fall into a defined class

Q22) Which QoS mechanism must be enabled for **map-class** to start?

A) LFI

B) LLQ

C) CAC

D) traffic shaping

Q23) What is the purpose of the **class class-default** command?

A) defines the voice signaling and traffic class maps

B) defines how the link resources are assigned to the map classes

C) assigns a queue for voice signaling traffic

D) defines how to classify traffic that does not fall into a defined class

Q24) During VoIP over PPP configuration, which command must be set properly for the correct fragment size to be calculated?

A) bandwidth

B) fragment-delay

C) class voice-traffic

D) ip precedence

Q25) What is the biggest advantage of using an automated policy tool such as CiscoWorks QPM?

A) It is less expensive than applying the policies manually.

B) It avoids inconsistencies in end-to-end policy application on a complex network.

C) It uses factory-recommended default settings for all devices.

D) It integrates well with all types of networks.

Q26) What type of information is supplied by the network-voice readiness report provided by QPM?

A) devices with software and hardware required to support QoS for voice

B) times of least congestion on the network

C) links that are best suited for transporting voice traffic

D) all of the above

Lesson: Call Admission Control

Q1) What may happen to data packets when the network is congested?

A) The packets are dropped.

B) The packets are queued.

C) The packets are buffered.

D) All of the above.

Q2) What is the function of CAC?

A) to deny traffic that does not meet overhead requirements

B) to deny traffic that has not been authenticated

C) to deny voice traffic if the required network resources are not available

D) to deny data traffic until higher priority voice traffic has been transmitted

Q3) How is traffic affected if a link is oversubscribed?

A) Data packets are corrupted.

B) Data packets are dropped.

C) Voice quality suffers.

D) All of the above.

Q4) If CAC and queuing is 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

Q5) 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

Q6) 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.

Q7) 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 look-ahead”

C) guarantees QoS against changing network conditions

D) knows how many other calls are active on the link

Q8) 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

Q9) What is the function of the **guaranteed-delay** command?

A) configures the **req-qos** and the **acc-qos** on the link

B) ensures that the reservation is made only if the **req-qos** is met

C) enables buffering of voice packets

D) ensures that the reservation is made only if the **acc-qos** is met

Q10) Which command is turned on by default when Cisco IOS Release 12.1(5)T is loaded?

A) ip rsvp bandwidth

B) guaranteed-delay

C) call rsvp-sync

D) req-qos

E) acc-qos

Q11) Put in correct order the steps for configuring RSVP with PPP.

___**Step 3**___1. Configure both **req-qos** and **acc-qos** using the **guaranteed-delay** command for RSVP to act as a CAC mechanism.

___**Step 1**___2. Turn on the synchronization feature between RSVP and H.323 using the **call rsvp-sync** command.

___**Step 4**___3. Use the **ip rsvp bandwidth** command to enable RSVP and specify the maximum bandwidth on the PPP interfaces that the call will traverse.

___**Step 2**___4. Configure RSVP on both the originating and terminating sides of the VoIP dial peers.

Q12) What is the **req-qos guaranteed-delay** command used for?

A) to specify required delay

B) to specify requested QoS

C) to request guaranteed delay

D) to request QoS services

Q13) The **max-conn** command is configured on _____.

A) the originating gateway

B) the terminating gateway

C) a dial peer of the outgoing gateway

D) a dial peer of the outgoing gatekeeper

Q14) Which situation is most suited to the use of the **max-conn** command to provide CAC?

A) when you want to limit the number of calls between sites

B) when you want to protect the bandwidth of the egress WAN link

C) when you want to protect the bandwidth of the ingress WAN link

D) when you have a large number of dial peers on the network

Q15) Which type of CAC mechanism involves sending probes to the destination IP address?

A) local CAC

B) measurement-based CAC

C) resource-based CAC

Q16) What type of information is typically compiled by measurement-based CAC techniques?

A) link bandwidth

B) loss characteristics

C) CPU power

D) available memory

E) delay characteristics

Q17) 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

Q18) Which device provides CAC for distributed call processing using CallManager?

A) DSP

B) dial peer

C) gatekeeper

D) gateway

Lesson: Voice Bandwidth Engineering

Q1) What are the 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) GoS

D) packet loss

Q4) What type of statistics are measured by the GoS?

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 GoS

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 to 16 percent the length of the call

D) 10 to 16 times the length of the call

Q9) What will be the busy hour traffic if the traffic for one month is 15,400 minutes?

A) 77 minutes

B) 105 minutes

C) 116 minutes

D) 119 minutes

Q10) The most accurate method of finding the busiest hour is to take _____ in a year, sum the traffic on an hourly basis, find the busiest hour, and derive the average amount of time.

A) the total number of days

B) the 10 busiest days

C) 22 business days

D) 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 type of arrival traffic can be modeled on a Poisson distribution?

A) random arrivals

B) smooth arrivals

C) bursty arrivals

D) all of the above

Q14) Regarding treatment of lost calls, which possibility overstates the number of trunks required?

A) LCC

B) LCD

C) LCH

Q15) What is the most commonly used table for calculating the number of physical trunks required?

A) Poisson distribution

B) Erlang B

C) GoS algorithm

D) LCC table

Q16) What are the 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) 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/from traffic matrix.

D) Use the A = C * T formula.

Q18) The call density matrix can be used to calculate the _____.

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

Q19) 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.

Q20) At what point can a voice and data network be said to have excessive load?

A) The averages demand over an 8-hour work day is 20 percent.

B) The average demand during the worst hour of the day is 30 percent.

C) The average demand over the worst 15 minutes of the day is 15 percent.

D) All of the above.

Module 8: Scalable Numbering and Applications

Lesson: Building a Scalable Numbering Plan

Q1) The North American telephone-numbering plan is based on _____ digits.

A) 3

B) 7

C) 10

D) 11

Q2) What type of information do you need to design a dial plan for a customer?

A) network topology

B) traffic-routing requirements

C) current dialing patterns

D) proposed router and gateway locations

E) all of the above

Q3) 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 **(E)**

_____ 2. makes the addition and deletion of number groups more manageable **(B)**

_____ 3. gives the network components the ability to focus on specific tasks to complete calls **(A)**

_____ 4. is affected by network design, translation rules, and alternate paths **(D)**

_____ 5. keeps dial plans consistent on the network by using translation rules to manipulate the local digit dialing patterns **(C)**

Q4) 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

Q5) 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 **(D)**

_____ 2. provides the ability to add new groups and modify existing groups easily **(A)**

_____ 3. controls number groups from a single point in the overall network **(E)**

_____ 4. establishes a group of numbers in a specific geographical area or functions group **(C)**

_____ 5. keeps local calls local and uses a specialized number key such as an area code for long distance calls **(B)**

Q6) 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

Q7) 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

Q8) Which worldwide prefix scheme was developed by ITU to standardize numbering plans?

A) G.114

B) E.164

C) G.164

D) E.114

Q9) Choose two locations where you can enter technology prefix commands. (Choose two.)

A) PBXs

B) gatekeepers

C) gateways

D) key systems

Q10) Technology prefixes can be used to identify _____.

A) type of gateway

B) class of gateway

C) pool of gateways

D) all of the above

Lesson: Applications

Q1) Hoot and Holler requires that _____ be enabled on the router.

A) SPRT

B) IP Multicast

C) IGRP

D) IGMP

Q2) Which modern technology have Hoot and Holler systems evolved into?

A) dial-on-demand

B) Advanced Peer-to-Peer Networking

C) B-ISDN

D) specialized leased-line

Q3) Toll bypass allow some ISPs to offer residential customers free or very low-cost _____.

A) Internet Access

B) software

C) long distance voice calls

D) bundled services

Q4) When customers are using toll bypass, which type of network is used for their long-distance voice calls?

A) PSTN with TDM-based switches

B) packet network with routers

C) PSTN with edge voice gateways

D) packet network with TDM-based routers

Q5) In the case of a hotel, a building or campus is wired with a _____ to supply voice, video, and Internet applications to the guest room.

A) LAN

B) ATM

C) 802.11 network access points

D) single broadband access line

Q6) Which two Cisco applications would you implement to provide hotel guests with access to room service and in-house events as well as airline flight status and weather updates? (Choose two.)

A) BBSM

B) Cisco IP Phone

C) Cisco ICS

D) CTI

E) CTE

F) Cisco IP AutoAttendant

Q7) Centrex is regarded as an _____ of telephony call services.

A) outdated mode

B) outsourcing

C) outplacement

D) outside network

Q8) Which two call control functions are provided by Centrex? (Choose two.)

A) billing services

B) CAC

C) authentication and authorization

D) RTP

E) dial tone

Q9) Which services can building owners deploy using multitenant applications?

A) VoIP

B) cable television

C) IP data services

D) all of the above

Q10) Multitenant applications allow building owners to deploy low-cost services to tenants in a common _____.

A) area code

B) ATM Infrastructure

C) campus or building

D) television viewing area

Q11) The Cisco VIA solution includes two key features and attributes such as _____ and _____. (Choose two.)

A) card recharging

B) sports scores

C) balance transfer

D) paging

E) automatic redial

Q12) Which type of network offers the least expensive option for prepaid and postpaid calling card services?

A) switched-circuit network

B) TDM-based network

C) packet voice network

D) none of the above

Q13) CTI applications allow users to perform tasks such as retrieving customer information from a database based on information provided by the _____.

A) caller ID

B) CTI server

C) amateur radio network

D) satellite system

Q14) Which CTI application can selectively handle incoming calls and help users make outgoing calls?

A) Cisco IP SoftPhone

B) Cisco IP Auto Attendant

C) Cisco IP Phone

D) Cisco WebAttendant

E) Personal Assistant

Q15) Two collaborative computing applications include _____ and _____. (Choose two.):

A) Microsoft Excel

B) Microsoft NetMeeting

C) Linux 7.3

D) IBM Lotus Notes

E) HTML applications

Q16) What is the function of collaborative computing?

A) allows team members to interact on a web page

B) allows team members in the same physical location to share resources and applications

C) allows team members to share resources and applications “in real time” regardless of their physical location

D) allows team members to develop spreadsheet applications such as Microsoft Excel

Q17) Which type of documents can Cisco AS5400 Series Universal Gateways interpret?

A) HTTP

B) WordStar

C) text

D) VoiceXML

Q18) At what location in the network does Cisco AS5400 Series Universal Gateways execute VoiceXML application logic to provide unified communications services?

A) the edge of the network

B) on offloading servers

C) within the network

D) all of the above

Q19) Which service is NOT offered by traditional call center technology?

A) recognition of customer telephones

B) recognition of customer ID

C) ability to view customer data while on the call

D) ability to access customer account balance while on the call

E) ability to send e-mail to the customer while on the call

Q20) Which Cisco application with Internet access allows call center agents to respond to customer queries over a variety of channels?

A) Cisco IPCC

B) Cisco IVR

C) Cisco IP Phone

D) Cisco AS5400 Series Universal Gateways

Q21) Which legacy devices does Cisco Unity integrate with in order to leverage existing communications infrastructure investments?

A) desktops

B) routers

C) trunks

D) PBXs

Q22) Which feature of Cisco Unity allows message interchange between disparate voice messaging systems?

A) Cisco Unity Bridge

B) AMIS-A

C) Avaya

D) Octel

B

Course Glossary

The Course Glossary for CVOICE v4.1 highlights and defines key terms and acronyms used throughout this course. Many of these terms are also described in the Cisco Internetworking Terms and Acronyms resource:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
3DES	Triple Data Encryption Standard	A stronger form of the Data Encryption Standard (DES), 3DES follows a pattern of encryption/decryption/encryption. 3DES has many different variations.
AAL1	ATM adaptation layer 1	One of four AALs recommended by the ITU-T. AAL1 is used for connection-oriented, delay-sensitive services requiring constant bit rates, such as uncompressed video and other isochronous traffic.
ABR	available bit rate	QoS class defined by the ATM Forum for ATM networks. ABR is used for connections that do not require timing relationships between source and destination. ABR provides no guarantees in terms of cell loss or delay, providing only best-effort service. Traffic sources adjust their transmission rate in response to information they receive describing the status of the network and its capability to successfully deliver data.
Ad-Hoc conference		A conference call feature where a conference is started by an initiator and only the initiator of the conference can add people into the conference.
ADPCM	adaptive differential pulse code modulation	A wave form process by which analog voice samples are encoded into digital signals.
AF	Assured Forwarding	A means of providing different levels of forwarding assurances for IP packets. This method is used by providers who offer differentiated services to their customers.
AIM	advanced integration module	A module in some Cisco routers that provides enhanced processing capabilities to the routers.
AMI	alternate mark inversion	Line-code modulation type used on T1 and E1 circuits. In AMI, marks (or ones) cause a pulse in alternating positive and negative directions, while zeroes never pulse. Two pulses of the same polarity are not allowed. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. Sometimes called *binary coded alternate mark inversion*.
ANI	automatic number identification	SS7 (Signaling System 7) feature in which a series of digits, either analog or digital, are included in the call, identifying the telephone number of the calling device. In other words, ANI identifies the number of the calling party.
ANSI	American National Standards Institute	A voluntary organization composed of corporate, government, and other members that coordinates standards-related activities, approves U.S. national standards, and develops positions for the United States in international standards organizations. ANSI helps develop international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO).
APC	adaptive predictive coding	A narrowband analog-to-digital conversion technique employing a one-level or multi-level sampling system in which the value of the signal at each sample time is adaptively predicted to be a linear function of the past values of the quantized signals. APC is related to linear predictive coding (LPC) in that both use adaptive predictors. However, APC uses fewer prediction coefficients, thus requiring a higher bit-rate than LPC.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
API	application program interface	The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. A set of standard software interrupts, calls, and data formats that computer application programs use to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create the links that an application needs to communicate with the operating system or with the network.
AR	access rate	1. The maximum data rate of the access channel, typically referring to access to broadband networks and network services. 2. A Frame Relay term which addresses the maximum transmission rate supported by the access link into the network, and the port speed of the device (switch or router) at the edge of the carrier network. The AR defines the maximum rate for data transmission or receipt. See also CIR (committed information rate).
ARPA	Advanced Research Projects Agency	Research and development organization that is part of DoD. ARPA is responsible for numerous technological advances in communications and networking. ARPA evolved into Defense Advanced Research Projects Agency (DARPA), and then back into ARPA again (in 1994).
ARQ	admission request	A RAS admission message defined as an attempt by an endpoint to initiate a call.
AS5300		A series of Cisco gateways that provide reliable, scaleable and feature-rich data and voice gateway functionality. The Cisco AS5300 Series Universal Gateways include the Cisco AS5300 Access Server/Voice Gateway and the Cisco AS5350 Universal Gateway.
ATM	Asynchronous Transfer Mode	The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, Synchronous Optical Network (SONET), and T3.
BC	basic call	A call between two users that does not require Advanced Intelligent Network Release 1 features (e.g. a POTS call).
Bc	committed burst	Negotiated tariff metric in Frame Relay internetworks. The maximum amount of data (in bits) that a Frame Relay internetwork is committed to accept and transmit above the committed information rate (CIR).
Be	excess burst	Negotiated tariff metric in Frame Relay internetworks. The number of bits that a Frame Relay internetwork attempts to transmit after Bc is accommodated. Be data, in general, is delivered with a lower probability than Bc data because Be data can be marked as DE by the network.
BHCA	busy hour call attempts	A traffic engineering term that refers to the number of call attempts made during the busiest hour of the day.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
BLF	busy lampfield	A visual display of the status of all or some of your phones. Your BLF tells you if a phone is busy or on hold. Your BLF is typically attached to or part of your operator phone.
BRQ	bandwidth change request	RAS bandwidth control message sent by endpoint to gatekeeper requesting an increase/decrease in call bandwidth.
BVM	BRI voice module	An optional device providing four ISDN Basic Rate Interface (BRI) ports for connection to ISDN PBXs or private integrated services network exchanges (PINXs). The BVM has four ISDN BRI ports for voice traffic. Each BRI port supports two voice channels (ISDN B channels) and one signaling channel (ISDN D channel).
CAS	channel associated signaling	The transmission of signaling information in association with the voice channel. In T1 networks, CAS signaling often is referred to as “robbed-bit” signaling because the network is robbing user bandwidth for other purposes.
CatOS	Catalyst software	Software that runs on Cisco Catalyst switches.
CBR	constant bit rate	QoS class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery.
CBWFQ	class-based weighted fair queuing	Congestion management mechanism that extends the standard WFQ functionality to provide support for user-defined traffic classes.
CCIS	common channel interoffice signaling	A technology that uses a common link to carry signaling information for a number of trunks. CCIS is similar to ITU-T SS6 protocol that operated at low-bit rates (2.4, 4.8, and 9.6 K) and transmitted messages that were only 28 bits in length.
CCITT	Consultative Committee for International Telegraph and Telephone	Former name for the International organization responsible for the development of communications standards. Now called the ITU-T.
CCS	common channel signaling	Signaling system used in telephone networks that utilizes a statistical multiplexing protocol for signaling. A specified channel is exclusively designated to carry signaling information for all channels in the system. An example is ISDN or SS7
CDVT	cell delay variation tolerance	In ATM, a QoS parameter for managing traffic that is specified when a connection is set up. In CBR transmissions, CDVT determines the level of jitter that is tolerable for the data samples taken by the peak cell rate (PCR).
CELP	code excited linear prediction	Compression algorithm used in low bit-rate voice encoding. Used in ITU-T Recommendations G.728, G.729, G.723.1.
centum call seconds		Units used to measure traffic load. A CCS is $1/36^{th}$ of an erlang. The formula for a centum call second is the number of calls per hour multiplied by their average duration in seconds, all divided by 100.
CES	circuit emulation service	Enables users to multiplex or to concentrate multiple circuit emulation streams for voice and video with packet data on a single high-speed ATM link without a separate ATM access multiplexer.
CID	channel ID	Designates the Frame Relay subchannel ID for Voice over Frame Relay.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
CIR	committed information rate	The rate at which a Frame Relay network agrees to transfer information under normal conditions, averaged over a minimum increment of time. CIR, measured in bits per second, is one of the key negotiated tariff metrics.
Cisco AVVID	Cisco Architecture for Voice, Video and Integrated Data	Cisco AVVID is the architecture for Voice, Video and Integrated DataCisco AVVID includes three components: infrastructure, such as switches and routers; clients, such as IP phones, H.323 videoconferencing equipment, and PCs; and applications, such as call control, that use a common IP network
Cisco CallManager		Software-based call- processing agent. It is a component of the Cisco IP telephony solution, part of Cisco AVVID (Architecture for Voice, Video and Integrated Data). The software extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, Voice over IP (VoIP) gateways, and multimedia applications.
Cisco.com		The name of Cisco Systems external Web site.
Cisco ICM software	Cisco Intelligent Contact Management software	Software, which delivers an integrated suite of capabilities, that enables a company to interact with its customers via phone, Web, and e-mail across an enterprise of automatic call distributor (ACD), private branch exchange (PBX), interactive voice response (IVR), database, and desktop applications.
Cisco IOS		Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks while ensuring support for a wide variety of protocols, media, services, and platforms.
Cisco IPCC	Cisco IP Contact Center	An integrated suite of products that enables agents using Cisco IP Phones to receive both time-division multiplexing (TDM) and Voice over IP (VoIP) calls. The IPCC can be implemented in a single-site environment or integrated into an enterprise wide multisite contact-center.
Cisco IP Phone		The Cisco family of IP Phones provides a complete range of intelligent communication systems that use the data network while providing the convenience and ease-of-use of a business phone.
Cisco IP SoftPhone		A Windows-based application for the PC. Used as a stand-alone end station or in conjunction with the Cisco IP Phone, it provides mobility, directory integration, user interface, and a virtual conference room.
CLI	command-line interface	An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.
CLID	Calling Line ID	Information about the billing telephone number from which a call originated. The CLID value might be the entire phone number, the area code, or the area code plus the local exchange. Also known as Caller ID.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
CNG	comfort noise generation	While using VAD, the DSP at the destination emulates background noise from the source side, preventing the perception that a call is disconnected.
CO	central office	The local telephone company office to which all local loops in a given area connect and in which circuit switching of subscriber lines occurs.
“Codebook” excitation index		Used by the receiver to look up a set of excitation values. A codebook is a set of rules that helps to determine what conditions indicate a Cisco device fault.
CPE	customer premises equipment	Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at customer sites, and connected to the telephone company network. Can also refer to any telephone equipment residing on the customer site.
CRC	cyclic redundancy check	Error-checking technique in which the frame recipient calculates a remainder by dividing frame contents by a prime binary divisor and compares the calculated remainder to a value stored in the frame by the sending node.
cross-connect (adj.) cross connect (n, v)		Cross connect is a connection scheme between cabling runs, subsystems, and equipment, using patch cords or jumpers that attach to connecting hardware on each end. Cross-connection is the attachment of one wire to another, usually by anchoring each wire to a connecting block and then placing a third wire between them so that an electrical connection is made. The TIA/EIA-568-A standard specifies that cross-connect cables (also called patch cords) are to be made out of stranded cable.
CRTP	Compressed RTP	A type of header compression designed to reduce the IP/UDP/RTP headers to two bytes for most packets in the case where no UDP checksums are being sent, or four bytes with checksums.
CS-ACELP	Conjugate Structure Algebraic Code Excited Linear Prediction	CELP voice compression algorithm providing 8 kbps, or 8:1 compression, standardized in ITU-T Recommendation G.729 or G.729a
CTI	computer telephony integration	The name given to the merger of traditional telecommunications (PBX) equipment with computers and computer applications. The use of caller ID to retrieve customer information automatically from a database is an example of a CTI application.
DACS	digital access and crossconnect system	A digital crossconnect system that provides grooming, switching, and aggregation.
dB	decibel	Unit for measuring relative power ratios in terms of gain or loss. The rule of thumb to remember is that 10 dB indicates an increase (or a loss) by a factor of 10; 20 dB indicates an increase (or a loss) of a factor of 100; 30 dB indicates an increase (or a loss) by a factor of 1000.
DCD	data carrier detect	Signal from the DCE (modem or printer) to the DTE (typically your PC), indicating it (the modem) is receiving a carrier signal from the DCE (modem) at the other end of the telephone circuit.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
DCE	data communications equipment (EIA expansion) data circuit-terminating equipment (ITU-T expansion)	Devices and connections of a communications network that comprise the network-end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE.
DDS	dataphone digital service	A class of service that is offered by telecommunications companies to transport data rather than voice.
DE bits	discard eligible bits	Bits that are used to tag Frame Relay frames which are eligible to be discarded if the network gets congested.
delay budget		The maximum amount of delay in data, voice and video applications. The total end-to-end delay when engineering a VoIP implementation should not exceed the 150- to 200-millisecond delay budget.
Delay Dial		A signaling method in which the terminating side remains off hook until it is ready to receive address information. The off-hook interval is the delay dial signal.
DHCP	Dynamic Host Configuration Protocol	Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
dial plan mapper		Provides the mapping of IP addresses to telephone numbers. After enough digits are accumulated to match a configured destination pattern, the dial plan mapper maps the IP host to a telephone number.
dialup (adj, n) dial up (v)		Modem access. The use of a dial or push button telephone to create a telephone or data call. Dialup calls are usually billed by time of day, duration of call and distance traveled. It is a connection to the Internet, or any network, where a modem and a standard telephone are used to make a connection between computers.
dialup remote access server		A remote access server is computer hardware which resides on a corporate LAN and into which employees dial on the public switched telephone network to get access to their email and to software and data on the corporate LAN (for example, status on customer orders). Remote access servers are also used by commercial service providers, such as Internet Access Providers (ISPs) to allow their customers access into their networks. Remote access servers are typically measured by how many simultaneous dial-in users (on analog or digital lines) they can handle and whether they can work with cheaper digital circuits, such as T 1 and E 1 connections.
Digital T1/E1 Packet Voice Trunk Network Module		A flexible and scalable T1/E1 voice solution for Cisco 2600 and 3600 series multiservice Modular Access routers that supports up to 60 voice channels in a single network module.
Digital T1/E1 voice port adapter		A single-width port adapter, which incorporates one or two universal ports configurable for either T1 or E1 connection with high-performance digital signal processor (DSP) support for up to 24 to120 channels of compressed voice.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
DLCI	data-link connection identifier	Value that specifies a PVC or an SVC in a Frame Relay network. In the basic Frame Relay specification, DLCIs are locally significant (connected devices might use different values to specify the same connection at different ends of the network).
DNIS	Dialed Number Identification Service	Feature of trunk lines where the called number is identified; this called number information is used to route the call to the appropriate service. DNIS is a service used with toll-free dedicated services whereby calls placed to specific toll-free numbers are routed to the appropriate area within the company.
DP	dial pulse	A means of signaling that consists of regular momentary interruptions of a direct or alternating current at the sending end in which the number of interruptions corresponds to the value of the digit or character. In short, the old style of rotary dialing. Dial the number "5" and you will hear five "clicks."
DPNSS	Digital Private Network Signaling System	A common-channel message-oriented signaling protocol commonly used by private branch exchanges (PBXs).
drop and insert		Allows DS-0 channels from one T1 or E1 facility to be cross-connected digitally to DS-0 channels on another T1 or E1. By using this method, channel traffic is sent between a PBX and a CO PSTN switch or other telephony device, so that some PBX channels are directed for long-distance service through the PSTN while the router compresses others for interoffice VoIP calls. In addition, drop and insert can cross-connect a telephony switch (from the CO or PSTN) to a channel bank for external analog connectivity. Also called TDM Cross-Connect. See DACS
DRQ	disengage request	Message sent by the gateway to the gatekeeper during the process of a call. The gateway waits for the disengage confirmation (DCF) message before it sends the setup message to the new destination gatekeeper.
DS0	digital service level zero	Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX. Also, a single timeslot on an E1.
DSI	digital speech interpolation	An algorithm that analyzes voice channels for silence. It suppresses the voice bits to conserve packet-line bandwidth and inserts a code to indicate to the far end that these bits have been removed. Also, referred to as VAD (voice activity detection).
DSL	digital subscriber line	Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: Asymmetric DSL (ADSL), High-Data-Rate DSL (HDSL), Symmetrical DSL (SDSL), and Very High Data Rate DSL (VDSL). All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.
DSP	digital signal processor	An electronic circuit that compresses voice signals, generates tones, and decodes received compressions. DSPs can also emulate modems for purposes of FAX relay.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
DTE	data terminal equipment	Device at the user end of a user-network interface that serves as a data source, destination, or both. DTE connects to a data network through a DCE device (for example, a modem) and typically uses clocking signals generated by the DCE. DTE includes such devices as computers, protocol translators, and multiplexers.
DTMF	dual tone multifrequency	Tones generated when a button is pressed on a telephone to convey address signaling.
DTR	data terminal ready	EIA/TIA-232 circuit that is activated to let the DCE know when the DTE is powered up and not in test mode.
E&M	ear and mouth Earth and Magneto receive and transmit	1. Trunking arrangement generally used for two-way switch-to-switch or switch-to-network connections. Cisco analog E&M interface is an 8-pin modular connector that allows connections to PBX trunk lines (tie lines). E&M also is emulated on E1 and T1 digital interfaces. 2. A type of signaling traditionally used in the telecommunications industry. Indicates the use of a handset that corresponds to the ear (receiving) and mouth (transmitting) component of a telephone.
ECMA	European Computer Manufacturers Association	Group of European computer vendors who have done substantial OSI standardization work.
E lead		The wiring arrangement on an E&M circuit in which the signal side sends its signaling information.
ESF	Extended Superframe	Framing type used on T1 circuits that consists of 24 frames of 193 bits each, with the 193rd bit providing framing information and other functions. ESF is an enhanced version of SF.
ETSI	European Telecommunications Standards Institute	ETSI is a non-profit organization producing voluntary telecommunications standards used throughout Europe, some of which have been adopted by the EC as the technical base for Directives or Regulations.
FDM	frequency-division multiplexing	Technique whereby information from multiple channels can be allocated bandwidth on a single wire based on frequency. An example is DSL.
FIFO	first-in/first-out	Refers to a buffering scheme where the first byte of data entering the buffer is the first byte retrieved by the central processor unit (CPU). In telephony, FIFO refers to a queuing scheme where the first calls received are the first calls processed.
Flash memory		A special type of electrically erasable programmable read-only memory (EEPROM) that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern PCs have their basic input/output system (BIOS) stored on a flash memory chip so that it can be updated easily if necessary. Such a BIOS is sometimes called a flash BIOS. Flash memory is also popular in modems because it enables the modem manufacturer to support new protocols as they become standardized.
four-wire		One of two distinct types of audio interface (two-wire or four-wire). The four-wire implementation provides separate paths for receiving and sending audio signals, which consists of T, R and T1, R1 leads.
frame-forwarding		Mechanism by which frame-based traffic, such as HDLC and SDLC, traverses an ATM network.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
FRTS	Frame Relay traffic shaping	Queuing method that uses queues on a Frame Relay network to limit surges that can cause congestion. Data is buffered and sent into the network in regulated amounts to ensure that the traffic can fit within the promised traffic envelope for the particular connection.
FXO	Foreign Exchange Office	An FXO interface connects to the public switched telephone network (PSTN) central office. Cisco FXO interface is an RJ-11 connector that allows an analog connection at the PSTNs central office or to a station interface on a PBX.
FXS	Foreign Exchange Station	An FXS interface connects directly to a standard telephone and supplies ring, voltage, and dial tone. Cisco FXS interface is an RJ-11 connector that allows connections to basic telephone service equipment, keysets, and PBXs.
gatekeeper		1. The component of an H.323 telephony system that performs call address resolution, admission control, and subnet bandwidth management. 2. Telecommunications: H.323 entity on a LAN that provides address translation and control access to the LAN for H.323 terminals and gateways. The gatekeeper can provide other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways. A gatekeeper maintains a registry of devices in the multimedia network. The devices register with the gatekeeper at startup and request admission to a call from the gatekeeper.
gateway		An H.323 term which describes the component of a H.323 telephony network which translates between one technology and another, typically between traditional telephony and TCP/IP.
generic traffic shaping		Shapes traffic by reducing outbound traffic flow to avoid congestion by constraining traffic to a particular bit rate using the token bucket mechanism.
GRQ	gatekeeper discovery request	RAS gatekeeper discovery message sent by endpoint to gatekeeper.
HDB3	high density bit 3	A line coding method used to maintain synchronization by ensuring a sufficient number of binary ones. HDB3 is used on E1 circuits.
HDLC	High-Level Data Link Control	Bit-oriented synchronous data link layer protocol developed by ISO.
Hoot and Holler		A broadcast audio network used extensively by the brokerage industry for market updates and trading. Similar networks are used in publishing, transportation, power plants, and manufacturing.
HSRP	Hot Standby Router Protocol	Provides high network availability and transparent network topology changes. HSRP creates a hot standby router group with a lead router that services all packets sent to the hot standby address. Other routers in the group monitor the lead router, and if it fails, one of these standby routers inherits the lead position and the hot standby group address.
HTTP	Hypertext Transfer Protocol	The protocol used by web browsers and web servers to transfer files, such as text and graphic files.
Hyperterm software		Terminal emulation software.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
IETF	Internet Engineering Task Force	Task force consisting of over 80 working groups responsible for developing Internet standards
IMAP	Internet Message Access Protocol	Method of accessing e-mail or bulletin board messages kept on a mail server that can be shared. IMAP permits client e-mail applications to access remote message stores as if they were local without actually transferring the message.
IMT	Inter-Machine Trunk	A means to give service providers access to more favorable tariffs and rates. In Signaling System 7 (SS7) environments, Inter-Machine Trunks (IMTs) terminate bearer traffic on the voice gateways.
IN	Intelligent Network	A network that provides IP routing, quality of service (QoS), network access and control, and network management services.
IP	Internet Protocol	Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.
IP cloud		The area in which data travels through an IP network. Illustrated in diagrams as a cloud.
IP precedence		A 3-bit value in the type of service (TOS) byte used for assigning precedence to IP packets.
IP RTP priority		A Frame Relay feature that provides a strict priority queuing scheme on a Frame Relay permanent virtual circuit (PVC) for delay-sensitive data, such as voice.
ISDN	Integrated Services Digital Network	Communication architecture offered by telephone companies that permits customers to access digital networks to carry data, voice, and other source traffic.
ISUP	ISDN User Part	SS7 protocol layer that defines the protocol used to prepare, manage, and release trunks that carry voice and data between calling and called parties under the auspice of ISDN.
ITU	International Telecommunications Union	An organization established by the United Nations to set international telecommunications standards and to allocate frequencies for specific uses.
ITU-T	International Telecommunication Union Telecommunication Standardization Sector	International body that develops worldwide standards for telecommunications technologies. The ITU-T carries out the functions of the former CCITT.
IVR	interactive voice response	Term used to describe systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words or, more commonly, DTMF signaling. Examples include banks that allow you to check your balance from any telephone and automated stock quote systems.
IXC	inter-exchange carriers	Common carrier providing long-distance connectivity between local access and transport areas (LATAs). The three major IXCs are AT&T, MCI, and Sprint, but several hundred IXCs offer long-distance service in the United States.
JTAPI	Java Telephony Application Programming Interface	A call control model developed by Sun Microsystems.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
LDAP	Lightweight Directory Access Protocol	Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory.
LDCELP	Low-delay CELP	CELP voice compression algorithm providing 16-kbps, or 4:1 compression. Standardized in ITU-T Recommendation G.728.
LFI	link fragmentation and interleaving	A Cisco IOS feature that reduces delay on slower-speed links by breaking up large datagrams and interleaving low-delay traffic packets with the smaller packets resulting from the fragmented datagram.
line code		Electrical modulation scheme used by digital carrier systems. In North America, T1 uses AMI or B8ZS line coding. In other countries, E1 uses AMI or HDB3 line coding.
LLQ	Low Latency Queuing	Enables use of a single priority queue in conjunction with class-based weighted fair queuing. Typically, the priority queue only carries VoIP traffic. All other traffic is carried in the user defined queues of CBWFQ.
LPC	linear predictive coding	Voice coding that uses a special algorithm that models the way human speech works. Because LPC can take advantage of an understanding of the speech process, it can be efficient without sacrificing voice quality.
LRQ	location request	RAS location request message sent to request the gatekeeper contact information for one or more E.164 addresses.
LSB	least significant bit	The bit of a binary expression having the least value; or, representing the number of ones.
MC	multipoint controller	A required part of an MCU. The MC is the conference controller. The MC handles negotiation between all terminals to determine common capabilities and controls conference resources such as multicasting. The MC does not deal directly with any of the media streams.
MCSs	media convergence servers	An integral component of the Cisco IP Communications system. A high availability server platform for Cisco AVVID.
MCU	multipoint control unit	A component that manages videoconferences of three or more participants.
MDF	Main Distribution Frame	The point where all network related external services, IP equipment, and wiring converge within a building.
Meet-Me conference		A conference feature where everyone who dials the same Meet-Me number will join the conference together.
MEL CAS	Mercury Exchange Limited Channel Associated Signaling	A voice signaling protocol used primarily in the United Kingdom.
MGCP	Media Gateway Control Protocol	Protocol that helps bridge the gap between circuit-switched and IP networks. A combination of Internet Protocol Device Control (IPDC) and Simple Gateway Control Protocol (SGCP), MGCP allows external control and management of data communications devices, or "media gateways" at the edge of multiservice packet networks by software programs.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
MICA	Modem ISDN Channel Aggregation	Modem module and card used in the Cisco AS5300 universal access servers. A MICA modem provides an interface between an incoming or outgoing digital call and an ISDN telephone line; the call does not have to be converted to analog as it does with a conventional modem and an analog telephone line. Each line can accommodate, or aggregate, up to 24 (T1) or 30 (E1) calls.
Microsoft NetMeeting		Complete desktop Internet conferencing solution for all Windows users with multi-point data conferencing, text chat, whiteboard, and file transfer, as well as point-to-point audio and video.
M-lead		The wiring arrangement on an E&M circuit in which the trunking side sends its signaling information.
MLP	Multilink Point-to-Point Protocol	Method of splitting, recombining, and sequencing datagrams across multiple logical data links under the PPP protocol.
MOS	mean opinion score	A common benchmark used to determine the perceived quality of sound produced by specific codecs.
MP	multipoint process	Part of an MCU. The MP processes the media streams. It receives audio, video, or data bits from the endpoints for which it does the required mixing, switching, and other processing before distributing the stream to the videoconference participants.
MTP	media termination point	A Cisco software application. An MTP software device allows the Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.
multicast backbone		Multicast backbone of the Internet. It is a virtual multicast network composed of multicast LANs and the point-to-point tunnels that interconnect them.
NSAP	network service access point	Network address, as specified by ISO. An NSAP is the point at which OSI network service is made available to a transport layer (Layer 4) entity.
ODBC	Open Database Connectivity	Standard application programming interface for accessing data in both relational and nonrelational database management systems. Using this application programming interface, database applications can access data stored in database management systems on a variety of computers even if each database management system uses a different data storage format and programming interface.
off hook		Call condition in which transmission facilities are already in use. Also known as *busy*.
OMAP	operations, maintenance, administration, and provisioning	Telephony operations functions include monitoring and discovery of problems before they negatively impact service. Administration deals with billing, department cross-charges, accounting, and capacity management. The telephony maintenance function is quite similar to the data networking processes of fault isolation and correction. The final element, provisioning, is used to define services for individual subscribers.
on hook		1. Condition that exists when a receiver or a handset is resting on the switchhook, or is not in use. 2. Idle state (open loop) of a single telephone or private branch exchange (PBX) line loop.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
OOS	Out-of-Service	State of the call or trunk.
OPX	Off-Premises eXtension	A telephone line from a phone system that is terminated in a different building than the one in which the phone system resides.
OSI	Open Systems Interconnection	International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.
PAM	pulse amplitude modulation	Modulation scheme where the modulating wave is caused to modulate the amplitude of a pulse stream.
PBX	private branch exchange	Digital or analog telephone switches located on the subscriber premises and used to connect private and public telephone networks.
PCI	protocol control information	Control information added to user data to compose an OSI packet. The OSI equivalent of the term “header.”
PCM	pulse code modulation	Technique of encoding analog voice into a 64-kb data stream by sampling with 8-bit resolution at a rate of 8000 times per second.
PCMCIA	Personal Computer Memory Card Industry Association	A standard interface that connects any type of device to a portable computer. Developed by PCMCIA in the early 1990s.
PINX	private integrated services network exchange	A PBX or key system, which in a BRI voice application, uses QSIG signaling.
PLAR	Private, line automatic ringdown	Voice circuit that connects two single endpoints together. When either telephone handset is taken off-hook, the remote telephone automatically rings.
plar-opx	PLAR Off-Premises extension	Specifies a PLAR Off-Premises eXtension connection. Using this option, the local voice port provides a local response before the remote voice port receives an answer. On FXO interfaces, the voice port will not answer until the remote side answers.
PLL	phase-lock loop	A chip on a T1 or E1 module that provides clocking information.
POP	point of presence	In Operations Support System (OSS), a physical location where an interexchange carrier installed equipment to interconnect with a local exchange carrier (LEC).
POTS	plain old telephone service	Basic telephone service supplying standard single-line telephones, telephone lines, and access to the public switched telephone network.
PQ	priority queuing	PQ ensures that important traffic gets the fastest handling at each point where it is used. It was designed to give strict priority to important traffic.
PSQM	Perceptual Speech Quality Measurement	A technique used for measuring voice quality. It compares the received audio with the transmitted audio.
PSTN	Public Switched Telephone Network	General term referring to the variety of telephone networks and services in place worldwide. Sometimes called POTS.
PTT	Post, Telephone, and Telegraph	Government agency that provides telephone services. PTTs exist in most areas outside North America and provide both local and long-distance telephone services.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
PVC	permanent virtual circuit	Connections that are assigned but not connected until data is sent, thereby not using bandwidth when idle. A virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.
PVDM	packet voice digital signal processor module	Provides the ability to increase the voice processing capabilities within a single network module.
QoS	quality of service	Measure of performance for a transmission system that reflects its transmission quality and service availability. Congestion management features allow you to control congestion by determining the order in which packets are sent out an interface based on priorities assigned to those packets.
QSIG	Q Signaling	An inter-PBX signaling protocol for networking PBX supplementary services in a multi- or uni-vendor environment.
RAS	registration, admission, and status	Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signaling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.
RBOCs	regional Bell operating companies	Seven regional telephone companies formed by the breakup of AT&T. RBOCs differ from regional Bell holding companies (RBHCs) in that RBOCs do not cross state boundaries.
RBS	robbed-bit signaling	A technique by which a single bit in every DS0 bearer channel is "stolen" from every 6th frame. The stolen bit is then used to carry signaling information.
redirect server		A server that accepts a SIP request, maps the address into zero or more new addresses, and returns these addresses to the client. It does not initiate its own SIP request nor does it accept calls.
RFC	Request For Comments	Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the Internet Architecture Board (IAB) as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.
RISC	reduced instruction set computing	A microprocessor design that processes fewer and simpler instructions so that it can provide higher speed.
round robin (n) round-robin (adj)		An algorithm used to schedule processes in a fixed cyclic order. Simply put, it means to “take turns.”
RQNT	request notification	RAS message that instructs the gateway to watch for specific events.
RRQ	registration request	RAS message sent as a registration request.
RSVP	Resource Reservation Protocol	Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. Also known as Resource Reservation Setup Protocol.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
RTCP	RTP Control Protocol	Protocol that monitors the QOS of an IP RTP connection and conveys information about the on-going session.
RTP	Real-Time Transport Protocol	Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.
RTSP	Real Time Streaming Protocol	Enables the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds, such as live audio and video, and stored content, such as pre-recorded events. RTSP is designed to work with established protocols, such as RTP and HTTP.
SAP	Session Announcement Protocol	A protocol used to assist in the advertisement of multicast multimedia conferences and other multicast sessions, and to communicate the relevant session setup information to prospective participants.
SCCP	1. signaling connection control part	Software that provides an OSI network layer service to its users. It does not support intermediate routing.
	2. Skinny Client Control Protocol	The Cisco standard for real-time calls and conferencing over Internet Protocol (IP).
SCP	service control point	An element of an SS7-based Intelligent Network that performs various service functions, such as number translation, call setup and teardown, and so on.
SDLC	Synchronous Data Link Control	Systems Network Architecture (SNA) data link layer communications protocol. SDLC is a bit-oriented, full-duplex serial protocol that has spawned numerous similar protocols, including HDLC
SDP	Session Description Protocol	A protocol used to describe multimedia sessions in order to enable session announcement, session invitation, and other forms of multimedia session initiation.
SF	Super Frame	Common framing type used on T1 circuits. SF consists of 12 frames of 193 bits each, with the 193rd bit providing error checking and other functions. SF is superseded by ESF but is still widely used. Also called D4 framing.
signal ground		Refers to the common electrical reference point of a circuit.
SIMMs	single in-line memory modules	A small circuit board that can hold a number of memory chips.
SIP	session initiation protocol	Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.
SLA	service level agreement	An agreement between the Internet service provider (ISP) and the client that guarantees a certain level of data transmission over the network.
SMDS	Switched Multimegabit Data Service	High-speed, packet-switched, datagram-based WAN networking technology offered by the telephone companies.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
SMTP	Simple Mail Transfer Protocol	Internet protocol providing e-mail services.
SNR	signal/noise ratio	A measure of transmission quality. The ratio of good or usable data (signal) to bad or undesired (noise) on a line, expressed in decibels (dB).
SOHO	small offices/home offices	Networking solutions and access technologies for offices that are not directly connected to large corporate networks.
spanning tree (n) spanning-tree (adj)		Loop-free subset of a network topology.
SQL	Structured Query Language	International standard language for defining and accessing relational databases.
SRST	Survivable Remote Site Telephony	A feature on some Cisco routers that uses the Skinny protocol to provide call-handling support for the local IP phones if the WAN connection to the CallManager fails.
SS7	Signaling System 7	Standard CCS system used with Broadband ISDN (BISDN) and ISDN. Developed by Bellcore.
SSP	service switching point	Element of an SS7-based Intelligent Network that performs call origination, termination, or tandem switching.
STP	signal transfer point	Element of an SS7-based Intelligent Network that performs routing of the SS7 signaling.
STUN	serial tunnel	Router feature allowing two SDLC- or HDLC-compliant devices to connect to one another through an arbitrary multiprotocol topology (using Cisco routers) rather than through a direct serial link.
SVC	switched virtual circuit	Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic.
T1/E1		T1: The standard multiplexed 24-channel voice/data digital span line. Used predominantly in North America. Operates at a data rate of 1.544 Mbps. Digital WAN carrier facility. T1 transmits DS-1-formatted data through the telephone-switching network, using AMI or B8ZS coding. E1: Wide-area digital transmission scheme used predominantly throughout the world that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.
tabletop		A conference phone used on a conference room table.
TAPI	Telephony Application Programming Interface	A call control model developed by Microsoft and Intel.
TCAP	transaction capabilities application part	SS7 protocol layer that helps exchange noncircuit-related data between applications.
T-CCS	transparent common channel signaling	Feature that allows the connection of two PBXs with digital interfaces that use a proprietary or unsupported CCS protocol without the need for interpretation of CCS signaling for call processing. T1/E1 traffic is transported transparently through the data network and the feature preserves proprietary signaling. From the PBX standpoint, this is accomplished through a point-to-point connection. Calls from the PBXs are not routed, but follow a preconfigured route to the destination.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
TDM	time-division multiplexing	Technique in which information from multiple channels can be allocated bandwidth on a single wire based on preassigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.
time stamp (n) time-stamp (v)		A field in certain FastPacket formats that indicates the amount of time the packet has spent waiting in queues during the transmission between its source and destination nodes. Used to control the delay experienced by the packet.
two-wire		One of two distinct types of audio interface (two-wire or four-wire). With the two-wire implementation, full-duplex audio signals are transmitted over a single pair which consists of tip (T) and ring (R) leads.
UAC	user agent client	A client application that initiates the SIP request.
UAS	user agent server	A server application that contacts the user when a SIP request is received, and then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.
UDP	User Datagram Protocol	Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
U interface		The ISDN interface between the telco and the user, also known as the local digital subscriber line (DSL) loop.
VAD	voice activity detection	Used to statistically save bandwidth by not sending packets in the absence of speech. When enabled on a voice port or a dial peer, silence is not transmitted over the network, only audible speech. When VAD is enabled, the sound quality is slightly degraded but the connection monopolizes much less bandwidth.
VBR	variable bit rate	QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class.
VBR-NRT	variable bit rate non-real time	Subclass of VBR. Used for connections in which there is no fixed timing relationship between samples but that still need a guaranteed QoS.
VBR-RT	variable bit rate real time	Subclass of VBR. Used for connections in which there is a fixed timing relationship between samples.
V card		An electronic business card. V cards carry information such as name, telephone numbers, mail addresses, e-mail addresses and Universal Resource Locators (URLs).
VIC	voice interface card	A Cisco interface card used to connect the system to either the PSTN or to a PBX.
videoconference		A meeting between people in different locations, using audio and video. The simplest type of videoconference can involve transmission of static images between two locations; the most complex videoconferences can use full-motion video and high-quality audio between multiple locations.

Acronym or Term	Expansion of Acronym	Definition of Acronym or Term
VoATM	Voice over ATM	A technology that enables a router to carry voice traffic (for example, telephone calls and faxes) over an ATM network. When sending voice traffic over ATM, the voice traffic is encapsulated using a special AAL5 encapsulation for multiplexed voice.
VoD	video on demand	System using video compression to supply video programs to viewers when requested via ISDN or cable.
VoFR	Voice over Frame Relay	A technology that enables a router to carry voice traffic (for example, telephone calls and faxes) over a Frame Relay network. When sending voice traffic over Frame Relay, the voice traffic is segmented and encapsulated for transit across the Frame Relay network using FRF.12 encapsulation.
VoIP	Voice over IP	The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using a variety of signaling protocols.
VoIPovFR	VoIP over Frame Relay	Provides VoIP application interworking over an existing Frame Relay network. Can be used over point-to-point leased lines or a Frame Relay circuit; it does not require a full-fledged Frame Relay network or service.
VoX	Voice over X	Term that refers to nontraditional methods of carrying voice.
VPN	Virtual Private Network	Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.
WFQ	weighted fair queuing	Congestion management algorithm that identifies conversations (in the form of traffic streams), separates packets that belong to each conversation, and ensures that capacity is shared fairly between these individual conversations. WFQ is an automatic way of stabilizing network behavior during congestion and results in increased performance and reduced retransmission.
WIC	WAN interface card	A Cisco interface card that Connects the system to the WAN link service provider.
Wink Start		A method of E&M signaling. When the signaling leads indicate a change to an off-hook state, the other side must send a momentary *wink* (on-hook to off-hook to on-hook transition) on the correct signaling lead before the call signaling information can be sent by the sending side. After the call signaling information is received, the side that sent wink goes off-hook again when the subscriber answers and stays that way for the duration of the call.

C

Cisco Resources

Overview

The Cisco website, Cisco.com is a central source for all of your Cisco networking needs. It contains both general interest and specific technical information. Because Cisco.com provides many resources, it is important for you to learn how to quickly locate the information that you need.

Upon completing this module, you will be able to:

- Use Cisco.com reference material
- Use Cisco.com online search tools

Outline

The module contains these lessons:

- Cisco.com Reference Material
- Specialized Tools

Note This manual shows the Cisco website as it looked when the manual was printed. The site changes and is updated frequently. For this reason, we have avoided listing specific links where possible.

Cisco.com Reference Material

Overview

The Cisco web site, Cisco.com, has a variety of tools and resources that can help you with your networking tasks. Information is available on designing and configuring your network correctly, placing and managing orders for Cisco products and services, and supporting your network around the clock. This lesson shows you how to access some basic tools on Cisco.com.

Importance

Networks are complex, crucial system configurations, so it is important to have to quick access to the information necessary to effectively manage your network.

Note This manual shows the Cisco website as it looked when the manual was printed. The site changes and is updated frequently. For this reason, we have avoided listing specific links where possible. To get the most benefit from this module, you should become familiar with the current location of the documentation discussed.

Objectives

Upon completing this lesson, you will be able to:

- List the Cisco.com resources
- Choose the appropriate tool within Cisco.com
- List the resources available within the Technical Documentation
- Identify methods to research product information using the Product Documentation
- List the resources available with the Configuration Guides
- Identify information available in the Command Reference Guides

Learner Skills and Knowledge

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

- A knowledge of networking terms and concepts
- Familiarity with use of a Web browser

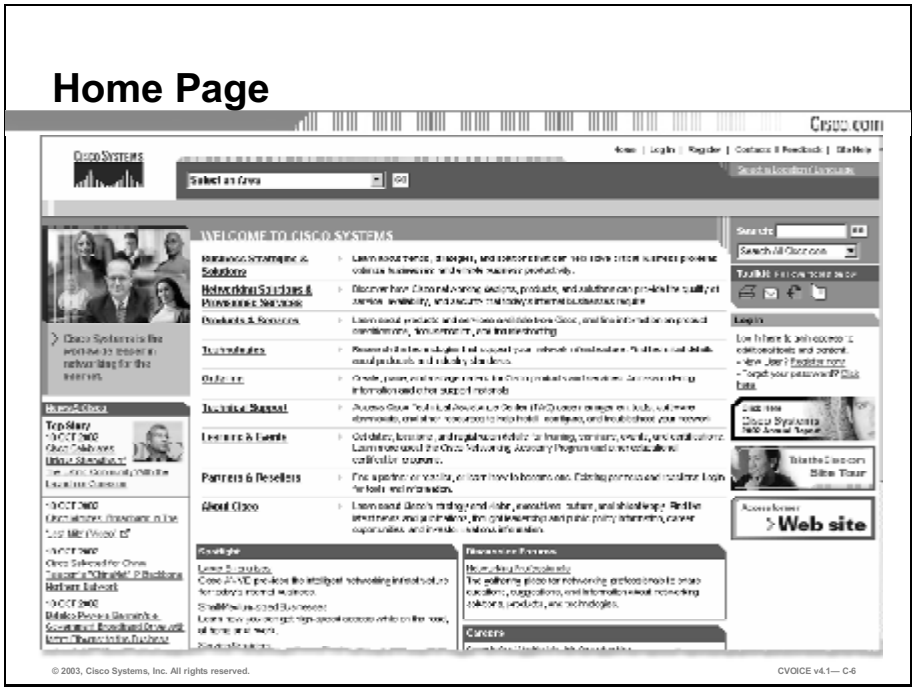
Outline

This lesson includes these sections:

- Overview
- Introduction to Cisco.com
- Choosing the Appropriate Tool
- Technical Documentation Section
- Product Documentation Section
- Configuration Guide
- Command Reference
- Summary
- Assessment (Quiz): Cisco.com Reference Material

Introduction to Cisco.com

While browsing the Cisco public website, you will find information of use to many different groups of Cisco users. In this section, you will learn to identify some of the resources available through Cisco.com.



The Cisco.com website can be found at: http://www.cisco.com. Some frequently used sections of general interest to Cisco.com visitors include:

- **Business Strategies & Solutions:** Offers end-to-end solutions from basic to advanced technologies. It includes information on planning, designing, implementing, and operating the solution.
- **Networking Solutions and Provisioned Services:** Contains links to descriptions of many Cisco networking designs, products, and solutions.
- **Ordering:** Allows visitors to buy equipment or software, find an authorized Cisco reseller, and order Cisco logo merchandise.
- **Learning & Events:** Provides information on the various Cisco certifications and exams and allows you to track your progress toward a certification. You can also locate Cisco Learning Partners and find out about Cisco-sponsored seminars, both live and online. Information about Networkers, the Cisco annual convention for networking technology professionals, is also available.

- **Online Discussion Forums:** the Cisco.com home page contains a direct link to the Networking Professionals Connection, where you can ask questions of an expert, or share your experiences with other networking professionals. You can also register to participate in live online presentations from this site.

- **About Cisco:** Offers public announcements about Cisco, such as job postings and corporate information.

In addition, links to recent news stories are directly on the home page, and various products or technologies are highlighted in the "Spotlight" section.

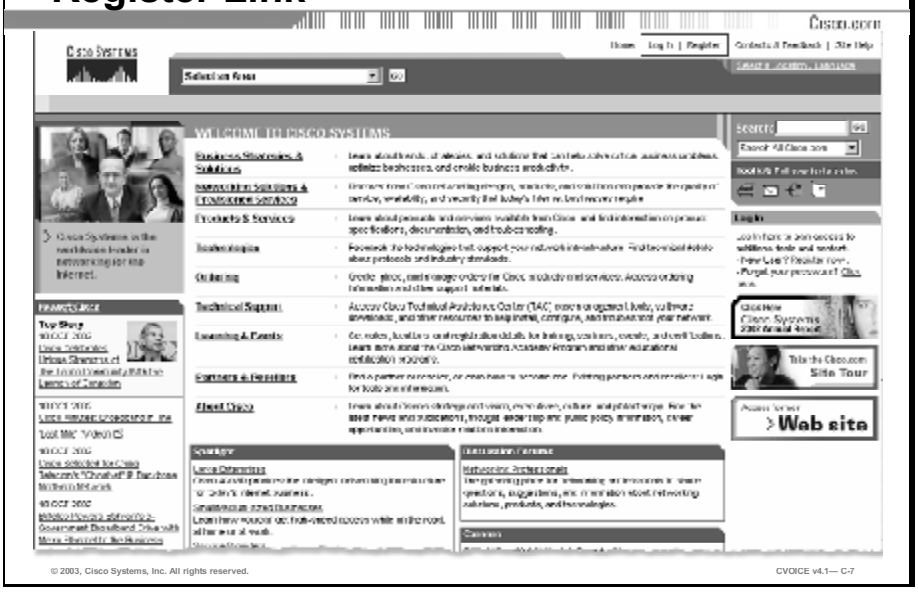
Additional technical information is also available through other sections of Cisco.com:

- **Products and Services:** Descriptions of Cisco products and services, product documentation, specifications, and troubleshooting information. Information is organized by product or service category, such as IOS Software, Switches, or Partner Support Services.

- **Technologies:** Technical information about networking protocols, technologies, and industry standards. Information is organized by protocol or technology, such as OSI, LAN, or QoS.

- **Technical Support:** This is a link to the Technical Assistance Center (TAC) website. It offers fast, 24/7 access to technical information. Users can obtain help with software, open a TAC case, report security incidents or product vulnerabilities, and manage product orders and support.

Register Link



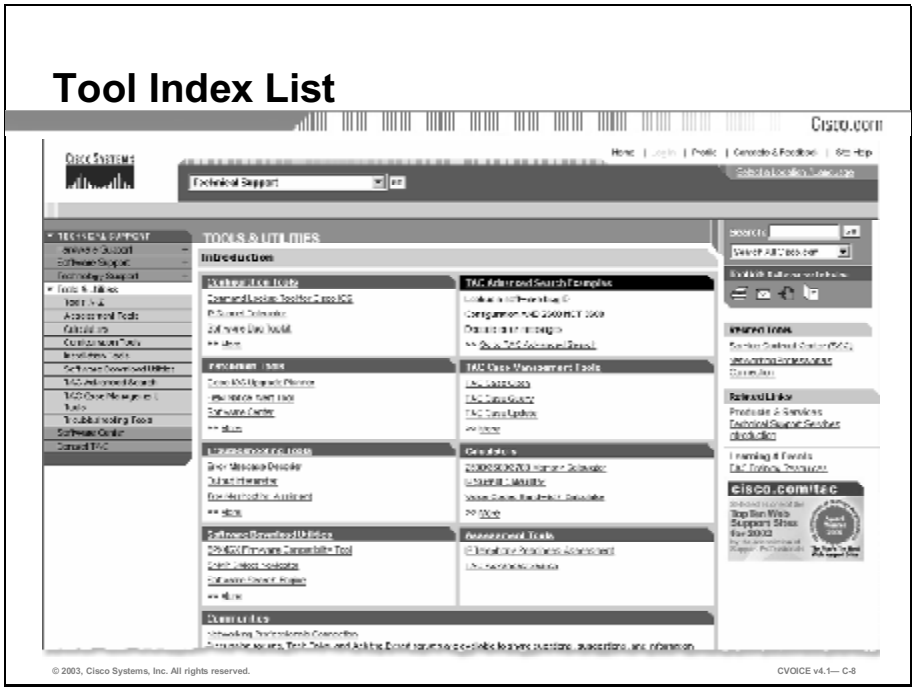
Much information is available to the general public on Cisco.com. However, to access all of the resources that Cisco offers, you will need to log in to the site. There are two levels of login access, Guest and Registered User.

A login at the guest level allows access to general company and product information. Registered access is for customers who have either purchased a support contract from Cisco or have been sponsored by a Cisco partner. This allows access to additional in-depth information and advanced online applications and services.

Create a Cisco.com login by clicking the “Register” link on the home page or by following a similar link on one of the other web pages of the site. Your access to information will vary based on the type of login you have.

Choosing the Appropriate Tool

Cisco.com contains many tools to help you get the technical information you need about equipment, software, protocols, and technologies. This section will help you choose the appropriate tool for your needs.



You have seen the various methods of accessing information from the Cisco.com home page. Although there are over 40 specific tools listed in the Cisco Tool Index, you can use the entire website itself to obtain the information that you need. This section describes some tools and utilities that are available on the Documentation CD as well as on Cisco.com. They include:

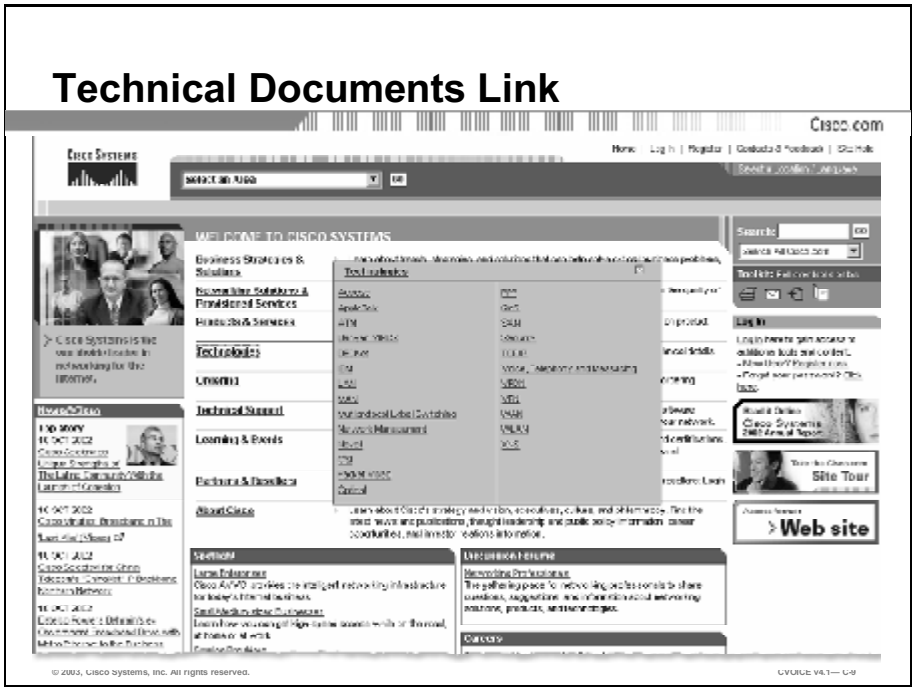
- Technical Documentation
- Product Documentation
- Configuration Guides
- Command References

Most of these resources are accessible in several different ways. The most direct way is usually from links on the Cisco.com home page, but there are also links on the Cisco TAC site. Frequently, pages offer links to other typically used tools and sections of the website. When you are exploring Cisco.com, be sure to pay attention to all of the options presented. Links to related information are often offered on the left or right side of the page.

Note Web page information is login specific.

Technical Documentation Section

In this section, you will become familiar with the resources available within the Technical Documentation section of the Cisco.com website.



The “Technologies” link on the Cisco.com home page brings up a pane listing several different networking technologies. Following any of these links will bring you to even more choices about the types of information that you can find. Links on the left side of the page take you to such areas as Overview, Protocols, Technical Details, Alerts and News, Implementation and Configuration Guides, and Relevant Products.

There is an additional link on the Cisco home page to Technical Documentation on Cisco.com Online. This site can be reached directly at http://www.cisco.com/univercd/home. The next figure shows the starting page of the Technical Documentation site, and the remaining part of this section will describe navigating from there.

Technical Documents Page

The Technical Documents link takes you to a web page with links to everything from a glossary of networking terms to descriptions of the latest technology. These white papers, books, and articles allow you to supplement your knowledge and keep up with the latest trends. You can also research possible network upgrades or changes. It is a good starting point for most of the documentation research commonly initiated.

At the top of the Technical Documents page is a cluster of cascading menus that are organized by major product categories. Making a choice from any of the menus at the top of the page will take you directly to the specific item within that category.

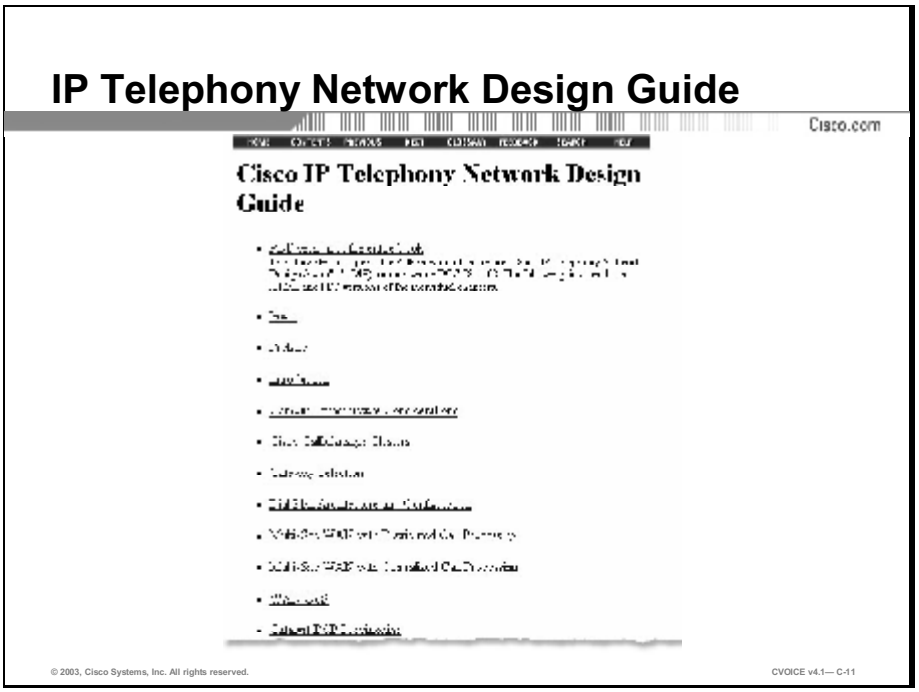
Directly below the menus are listings for various products that do *not* fit within the menu categories, such as hubs, digital subscriber line (DSL) and cable hardware, and router configuration utilities. The “Cisco Integrated Networking Solutions” link goes to descriptions of solutions such as Ipv6, Security Solutions, and Virtual Private Network (VPN) Solutions.

An area you may find helpful is the Networking Information category. Design guides and case studies are available to help your understanding of networking technologies. Troubleshooting guides can help in managing your network. Other categories provide even more resources, such as *Packet Magazine*, the Cisco systems user magazine.

Example

Suppose you are considering implementing Voice Over IP (VoIP) within your company. Choose “IP Telephony” from the “Voice/Telephony” category. This takes you to a page with links to technical documents on this subject.

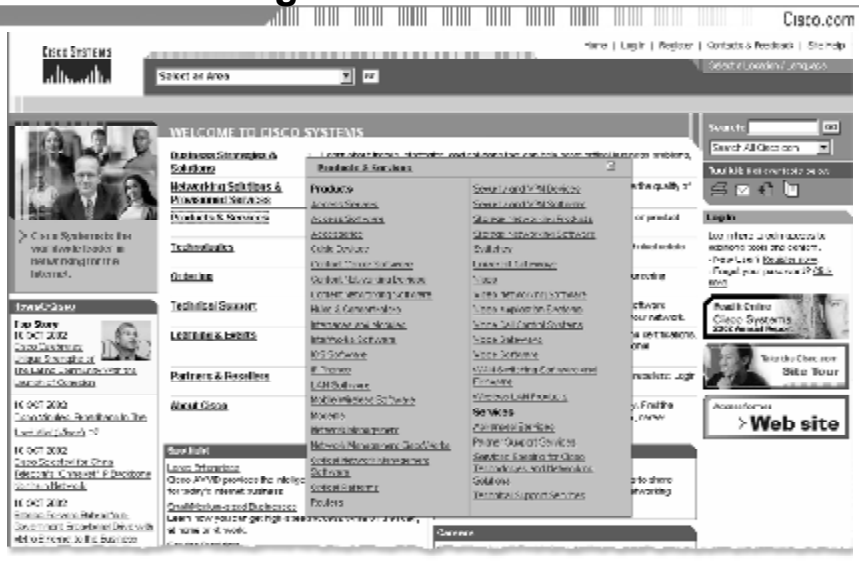
Choose the “IP Telephone Network Design Guide” to view an entire online book. This book explains the concepts and process of designing a VoIP network with examples of networks ranging from simple to complex. Additionally, many technical documents have links to further information.



Product Documentation

In this section, you will learn how to research product information using the Product Documentation available on Cisco.com. Product Documentation is available from the Cisco.com home page by using the links under the “Products and Services” section, or from the Technical Documents page.

Product Categories



Product Documentation Links

An important part of designing a new network, or upgrading an old network, is choosing the right equipment for the job. Cisco Product Documentation can help with that.

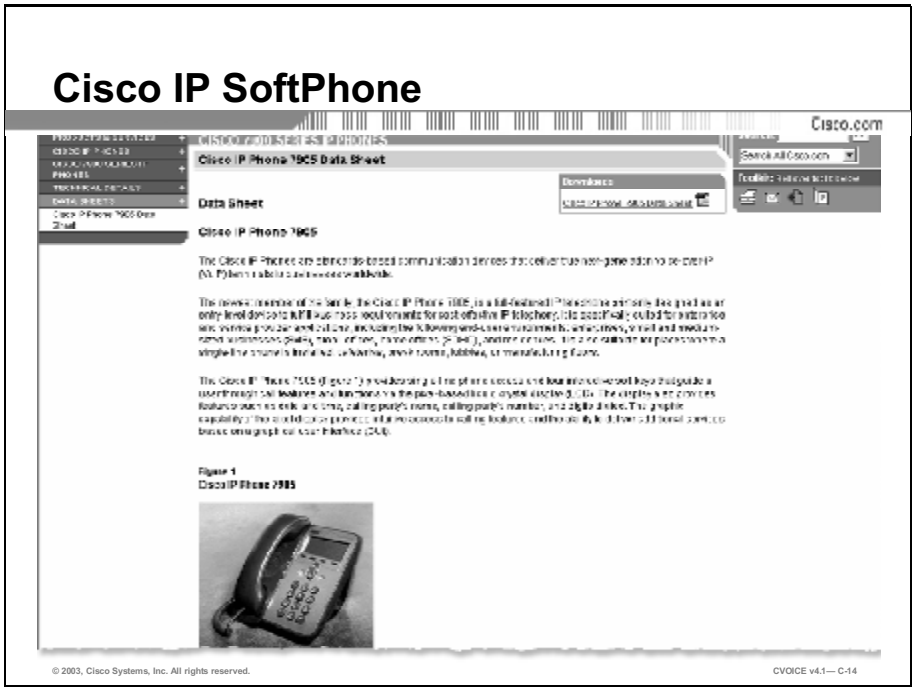
If you are interested in a specific type of product, the menu that appears when you click on "Products & Services" will link to the appropriate page. From there you can access information and documentation on that product or service. If you do not see the exact category you need, choose the Products & Services link at the top of the popup box. This link gives you access to an alphabetical Product index and a Service index, the entire Product Catalog, information on Product Warranties, Technical Documentation, and Network Optimization Support. Additionally, there are links to specific product categories.

From the product category site the standardized links on the left side of the page allow you to access information such as Technical Documentation, Instructions and Guides, and Product Support information. These links can assist you in choosing the appropriate Cisco products.

Cisco has introduced a Product Advisor that recommends Cisco networking hardware based on product features and high-level business requirements. This tool can be used in a novice, question-and-answer mode or in an expert, feature selection mode. Once products are recommended, you can compare them on a feature-by-feature basis. The Product Advisor can be reached at http://www.cisco.com/go/advisor, or from the Tool Index found on the Products & Services main page.

Example

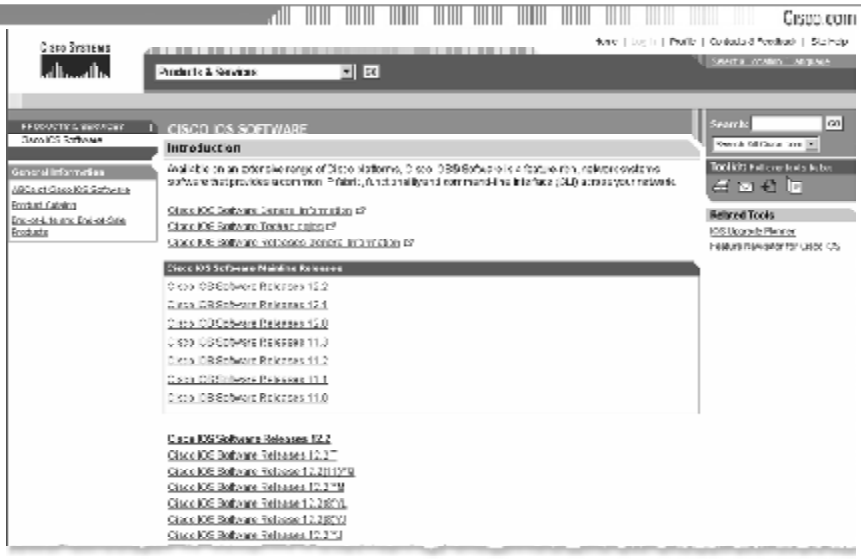
Suppose you are interested in IP telephones. You would choose “IP Phones” from the menu under “Products & Services” on the Cisco.com home page. Following the links from the IP telephone page takes you to information such as Data Sheets, Product Bulletins, and presentations on the different types of IP Phones offered by Cisco. The figure here represents one of the data sheet pages for the Cisco 7900 series IP Phones. Notice that there are links to more literature, products, and technical information. The links on the left side of the page provide a standard location for navigation within the category of IP Phones, and can also take you back to the main Products & Services page. There is a search function on the far right, and a Toolkit from where you can print the page, email it or reach a glossary.



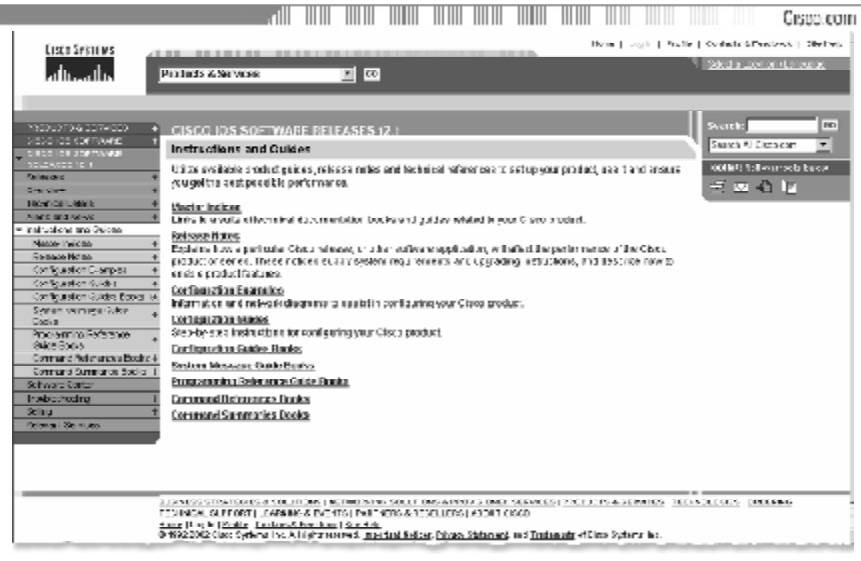
Configuration Guides

Configuring your Cisco equipment properly is crucial to getting the best use from it and to maintaining an optimally configured network. When you complete this section, you will be able to list the resources available within the Cisco Configuration Guides.

Cisco IOS Software Release 12.1 Link



Cisco IOS Software Release 12.1



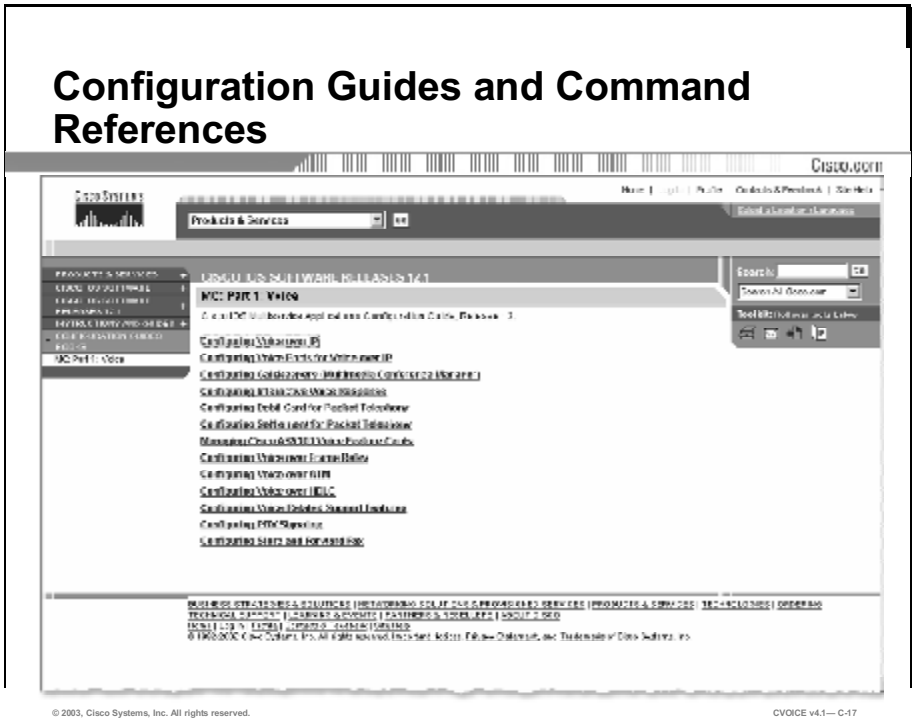
Whether you are working with new Cisco equipment or upgrading an existing network, you need to know how to configure the technologies and equipment in your network. The Configuration Guides have the information you need to do this. There are configuration guides for products and software—they can be reached from their pages within the Products & Services sections. There are also configuration guides for Cisco IOS software, which can be reached either from the Cisco IOS Software link in the Products & Services popup box, or from the Technical Documents page. The figure illustrates the path from the Cisco home page using the Products & Services link.

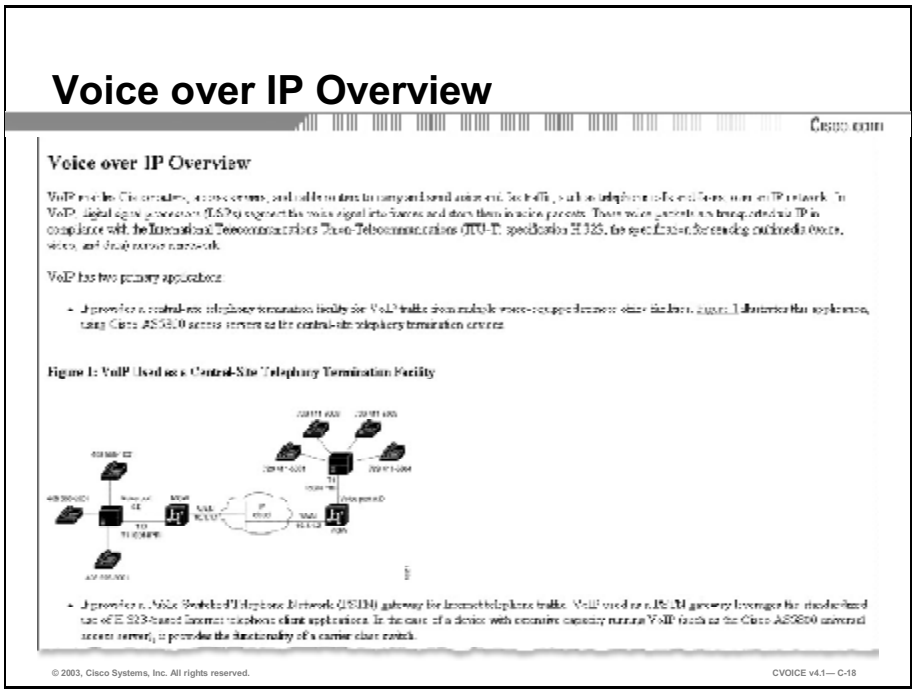
You might use this tool if you had upgraded your network to a new version of code and needed to learn the new options available to you. For example, if you need to implement an unfamiliar technology, such as changing to a different routing protocol. Each version of the Cisco IOS® software has its own complete set of helpful documentation.

The configuration guides available in this section describe protocols, explain technologies, and detail configuration tasks. They contain diagrams and comprehensive configuration examples from the most basic to the most advanced configurations.

Example

To reach the Configuration Guides from either the Cisco IOS Software page or the Technical Documentation page, choose the appropriate Cisco IOS software version from the menu; this takes you to the Documentation page for that Cisco IOS release. Notice that this page contains other information that might be of interest. If you have upgraded to a new Cisco IOS version, you may be especially interested in the “Alerts and News,” the “Release Notes,” and “Troubleshooting.” Additionally, there are Master Indices for the Configuration Guides and the Command References.





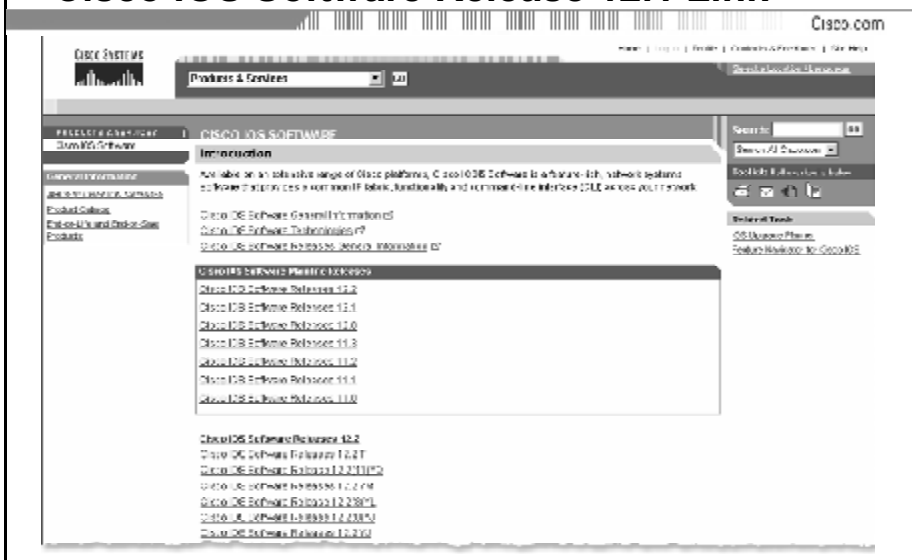
The next step is to select the “Configuration Guides Books” link. The various technologies that this version of the Cisco IOS software supports are grouped by type and subject.

Listed under the Configuration Guide for “Multiservice Applications” is a link for “Voice.” By following that link, you will be presented with a listing of all the configuration guides that meet your criteria; from here you can choose the exact configuration guide that you need. The figure illustrates an overview of configuring VoIP.

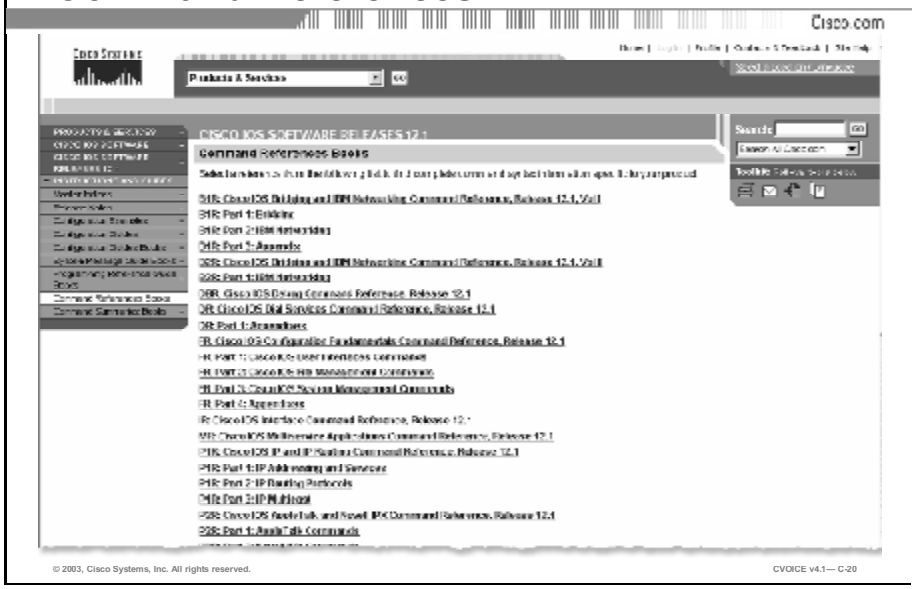
Command Reference

The full syntax and usage for each command is shown in the Command Reference Books. In this section, you will learn to use the Command Reference to look up command syntax.

Cisco IOS Software Release 12.1 Link



Command References



It would be impossible for anyone to memorize the exact syntax and all of the options for every command in the different versions of Cisco operating systems. For this reason, the Command Reference is an essential tool for every network engineer. This is also a good place to find a description and syntax for less common command options.

The Command Reference does not only list commands; it provides information about each command. You will find:

- A description of the command syntax and all of the available options
- Default values for any settings included in the command
- Command modes and command history
- Usage guidelines
- Examples of the command in use
- A list of, and links to, related commands

Example

One way to reach Command Reference is from the Cisco IOS Software link on the Products & Services popup box on the Cisco.com home page. It can also be reached via the Technical Documents page. Select the appropriate Cisco IOS version from the menu; the Instructions and Guides page for that software release opens. Notice that this page contains other information of interest. If you have upgraded to this Cisco IOS version, you may be especially interested in the "Alerts and News," the "Release Notes" or "Troubleshooting." There are also Master Indices for the Configuration Guides and the Command References.

For this example, choose the link for Command References Books. The commands are grouped by technology type. After selecting the appropriate technology category, follow the alphabetical links to the command you need. The figure shown illustrates what the Command Reference would look like if you were configuring a destination pattern for a voice peer.

To reach command documentation for the **destination-pattern** command, choose Cisco IOS Multiservice Applications Command Reference is from the Command Reference Book index. This link takes you to a page with an index of alphabetical groups of commands. Choose "Multiservice Applications Commands: C through D." All that remains is to scroll down to **destination-pattern** command and click on the link.

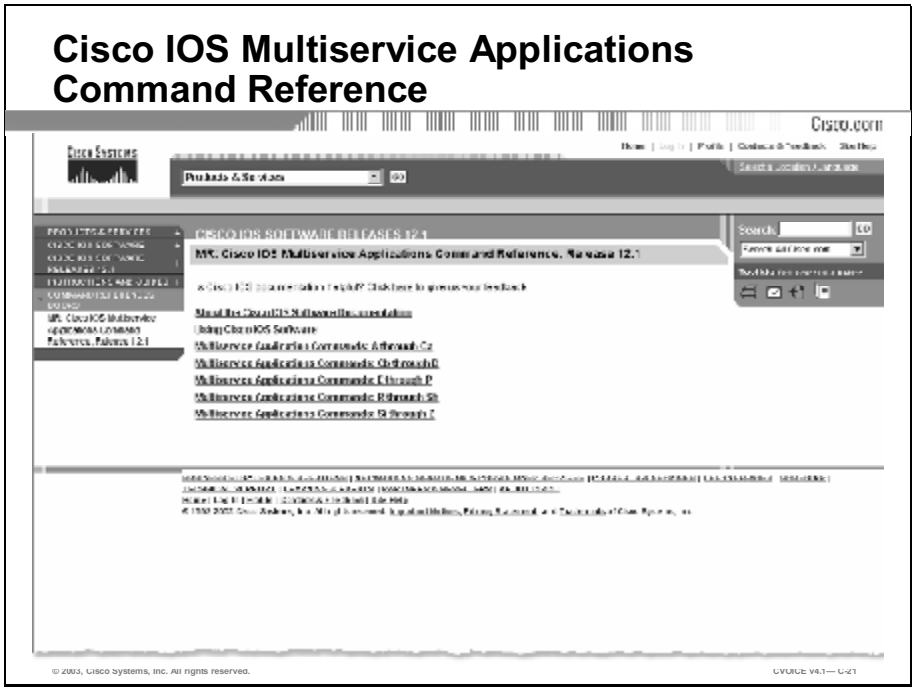
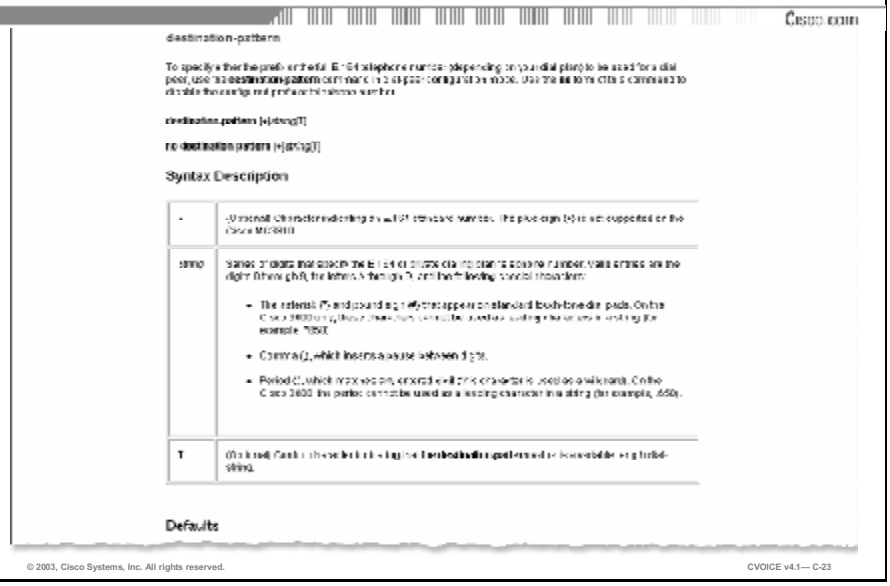


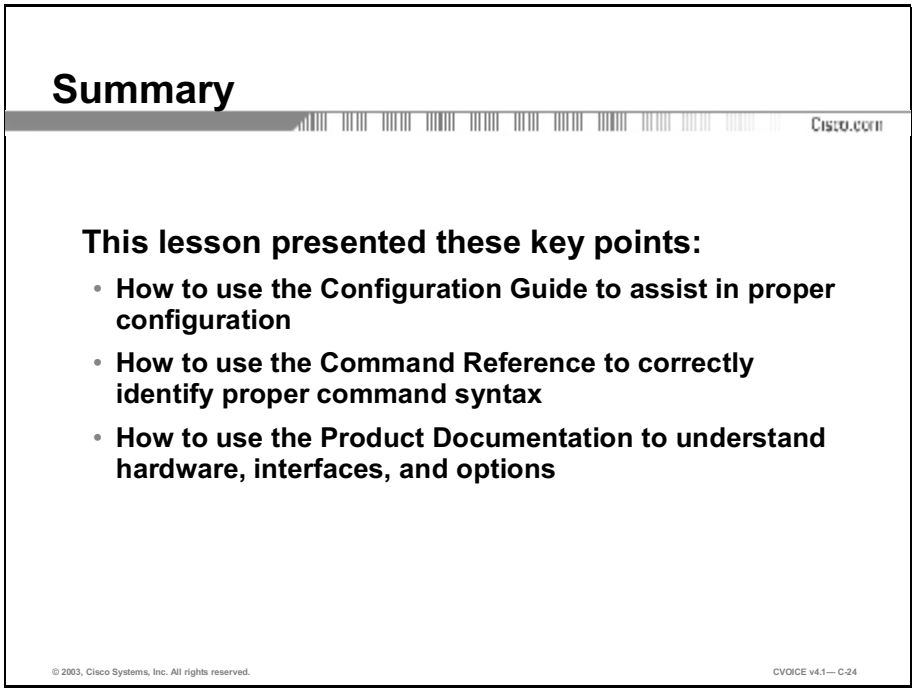
Table of Contents

Destination-Pattern



Summary

This section summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Cisco.com Reference Material
- Specialized Tools lesson

References

For additional information, refer to these resources:

http://www.cisco.com

Quiz: Cisco.com Reference Material

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Choose the appropriate Cisco.com tool for your needs
- Find the necessary information within the Cisco.com tool

Instructions

Answer these questions.

Q1) Match the tool to the task. You may use each tool more than once.

A) Technical Documents section

B) Configuration Guide Tool

C) Command Reference Tool

D) Product Documentation Tool

_____ 1. Find the correct syntax for a command

_____ 2. Learn the issues involved in configuring EIGRP in your network

_____ 3. See examples of Cisco IOS configurations

_____ 4. Choose the appropriate equipment needed for a network

_____ 5. Become familiar with the Documentation CD interface

_____ 6. Learn all the options for a command

_____ 7. Access product catalogs and literature

_____ 8. See release notes for a particular version of software

_____ 9. Learn about new Cisco products

_____ 10. Link quickly to documentation relating to various technologies

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

Specialized Tools

Overview

In this lesson you will examine some of the more advanced specialized tools available on the Cisco public website, Cisco.com. These tools will help you research software releases and upgrades, track bugs, download software, and access the wide-ranging support that is available in the Technical Assistance Center (TAC).

Importance

Some of the main reasons why Cisco customers, as well as prospective customers, access Cisco.com are to obtain Cisco IOS software upgrades and learn more about the Cisco range of software products. Additionally, knowing how to use the TAC helps you troubleshoot problems and occasionally saves you from having to open a TAC case.

Note	This manual shows the Cisco website as it looked when the manual was printed. The site changes and is updated frequently. For this reason, we have avoided listing specific links where possible.

Objectives

Upon completing this lesson, you will be able to:

- Use the Software Advisor tool to discover product features and Cisco IOS releases
- Use the Bug Toolkit to research Cisco IOS bugs and fixes/workarounds
- Use the Software Center to download appropriate software releases

- Use the TAC section of Cisco.com to research configuration issues and challenges

Learner Skills and Knowledge

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

- Knowledge of basic networking terms and concepts
- Familiarity with use of a Web browser

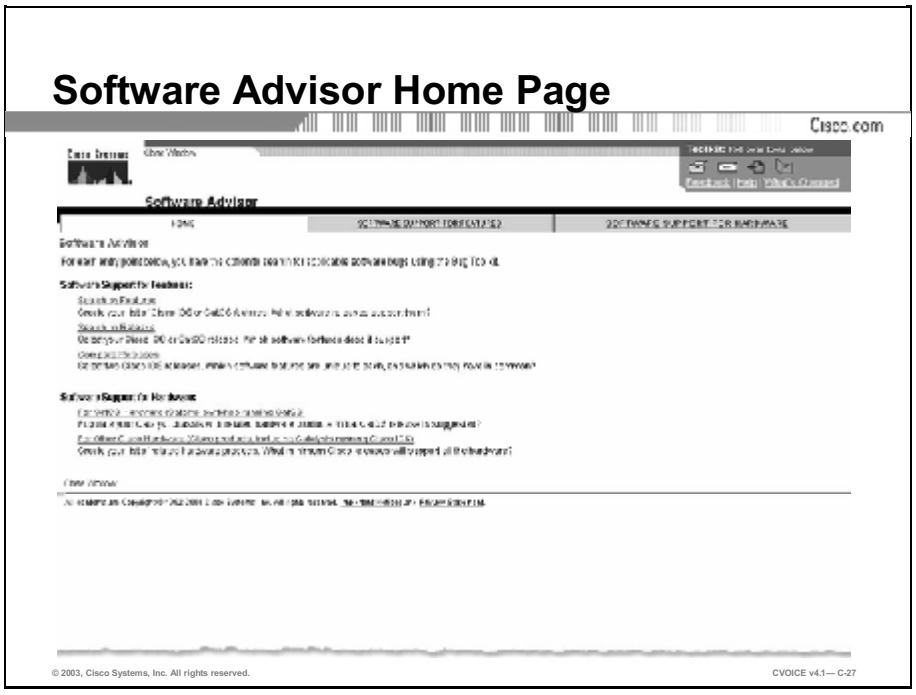
Outline

This lesson includes these sections:

- Overview
- The Software Advisor Tool
- Bug Toolkit
- Software Center
- Search the TAC Online
- Summary
- Assessment (Quiz): Specialized Tools
- Assessment (Complex Lab): Lab Exercise 1-1

The Software Advisor

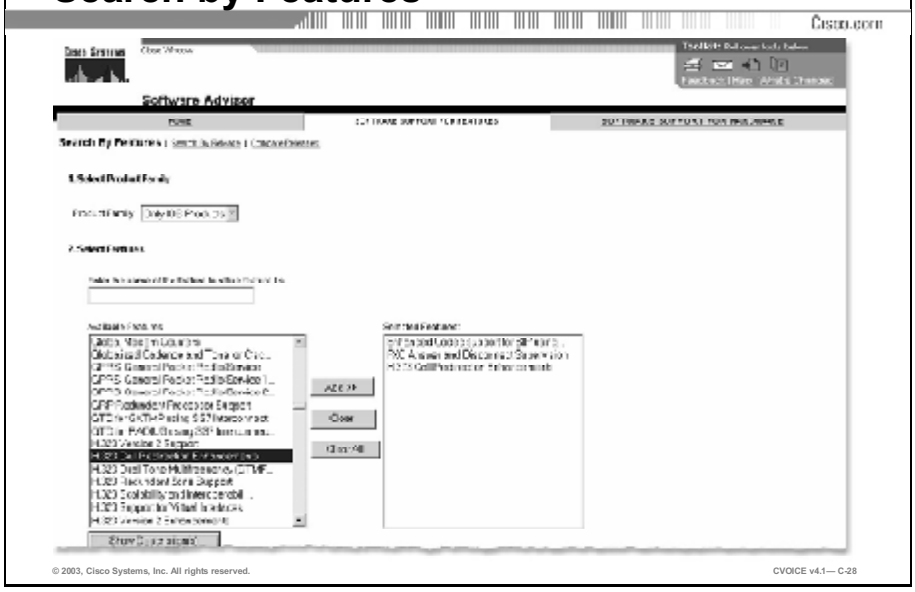
You can use Cisco Software Advisor to compare Cisco IOS® releases, match Cisco IOS and Catalyst OS features to releases, and find out which software release you need to support your hardware. This section explains how you can use the Software Advisor to effectively choose Cisco software.



The Software Advisor allows you to research Cisco IOS and CatOS software based on many different categories from one central location. You can search based on:

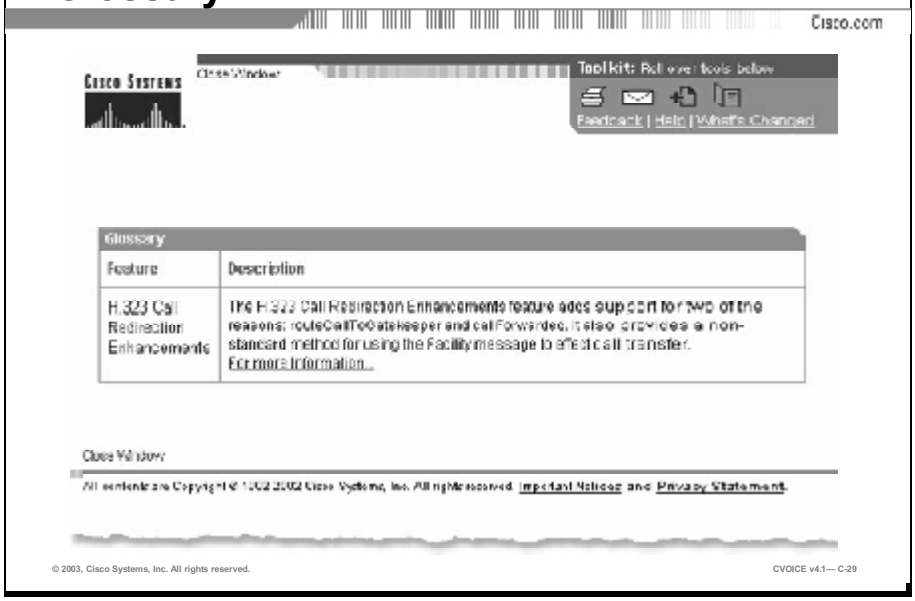
- Software:
  - Search by Features
  - Search by Release
  - Compare Releases
- Hardware:
  - CatOS products that run the CatOS
  - All other Cisco hardware

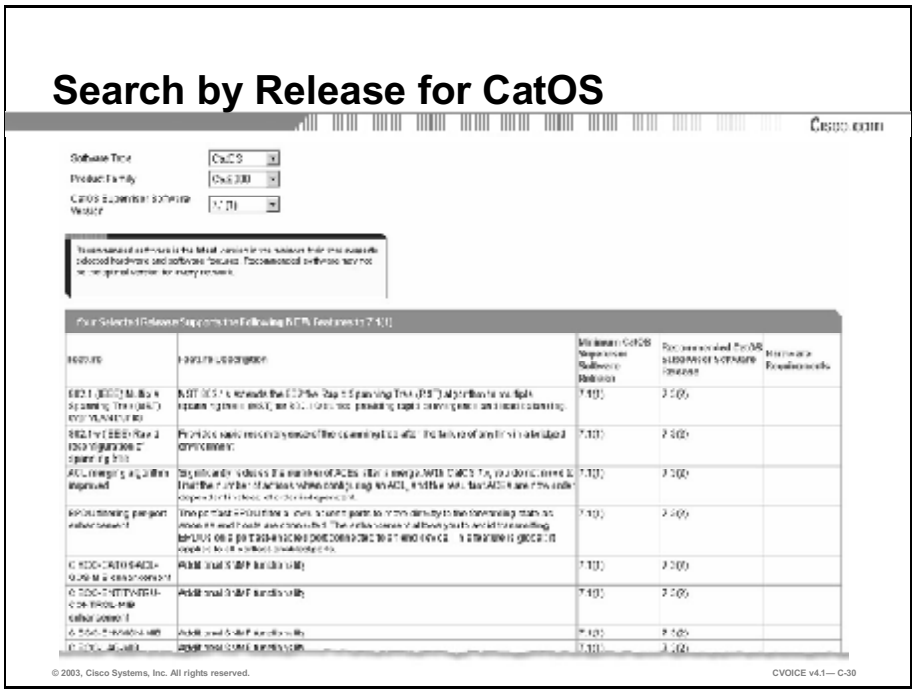
Search by Features



When you choose to Search by Features, you can narrow your choice based on the product line. When a comprehensive list of features appears, you can choose a group of features to search. If you are unsure of the meaning of a particular category, you can use the “Show Description” link for additional information. By working your way through the Advisor and narrowing down your choices at each junction, you can find the software containing the features that you need.

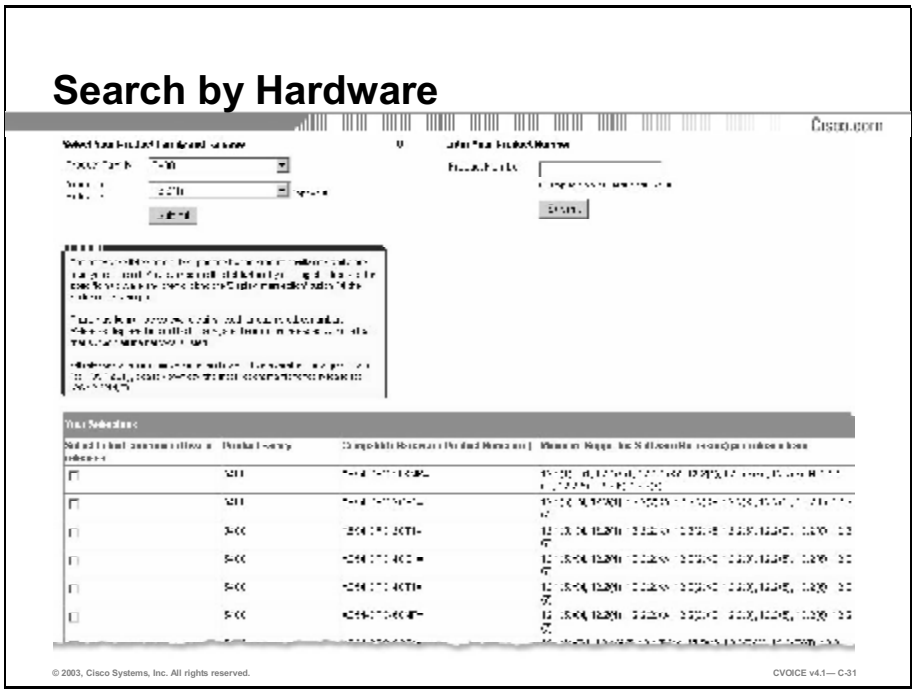
Glossary





Searching the software database by release gives you information based on the release version of either the CatOS or the Cisco IOS software that you are researching and on your specific hardware platform.

Comparing Releases allows the comparison of two Cisco IOS releases. You can specify the major release version, the maintenance release number within the version, the hardware platform, and the feature set in which you need to search. The result is a side-by-side comparison of the two releases, enabling you to make an informed choice between the releases. To view the output of a comparison between two software images, see the example section of this lesson.

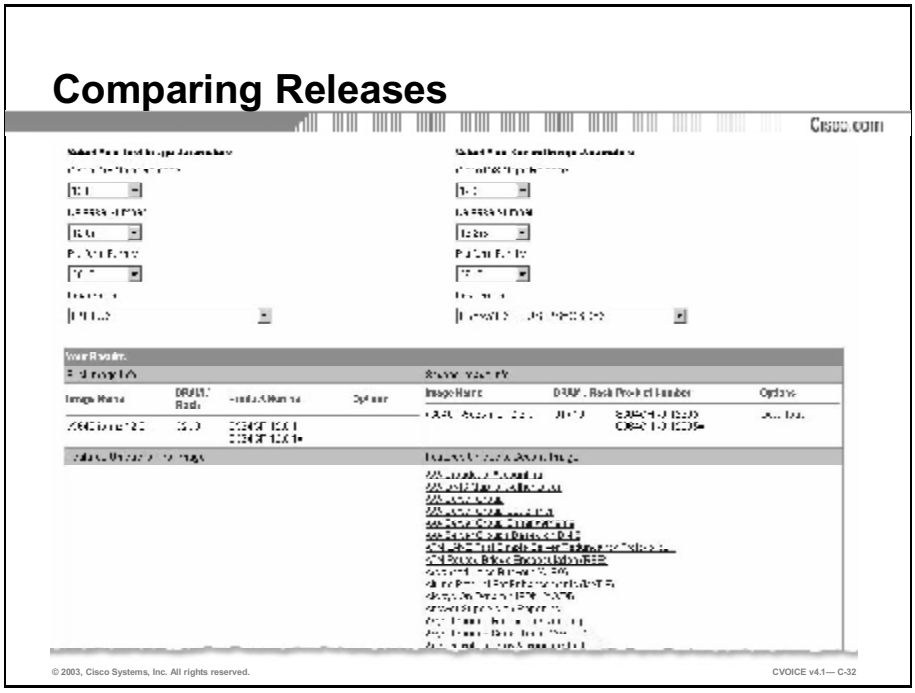


Searching by hardware takes a slightly different approach depending on whether you are searching for Cisco IOS or CatOS products. For Cisco IOS, entering either the product family or product number will return a table that lists the hardware and software supported by that product. The CatOS search engine leads you through specifying the exact hardware and modules and then recommends a Supervisor software version.

You can reach the Software Advisor from the “Products & Services” link on the Cisco.com home page, from the Tool Index, or from the “Installation Tools” link under the “Tools and Utilities” section of the TAC home page, as well as from many other Cisco.com sites dealing with software issues.

Example

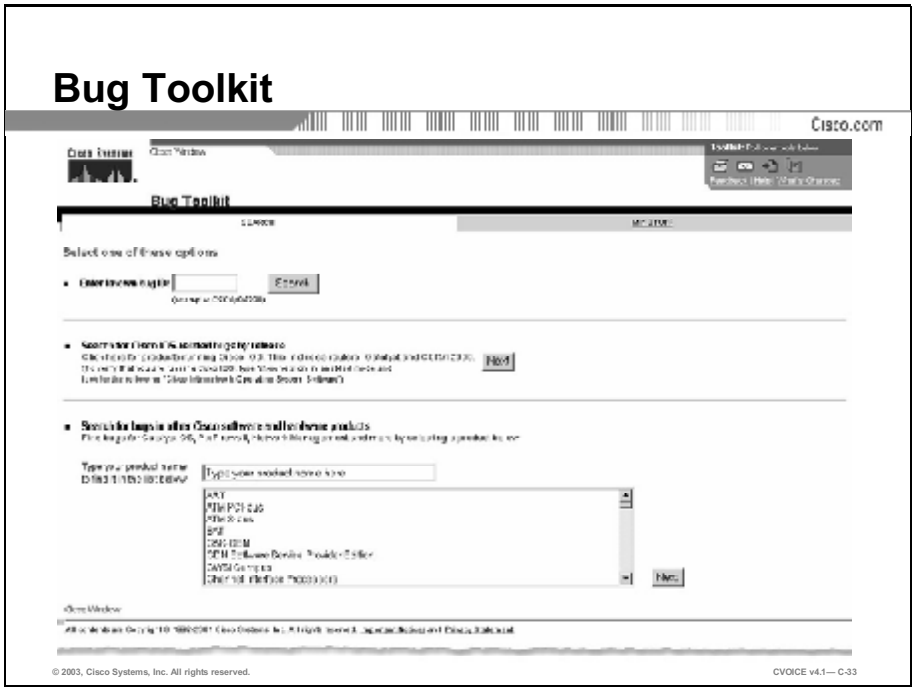
Suppose you are considering upgrading a Cisco 3640 router to a new Cisco IOS release. If you need to see what additional functionalities are available, choose “Compare Releases” from the Software Advisor home page. Then you need to specify the release number and the router model number. For this example, suppose that you have version 12.0(1), IP Plus feature set. You need to consider version 12.2(5), IP/FW/IDS Plus IPSEC 3DES.

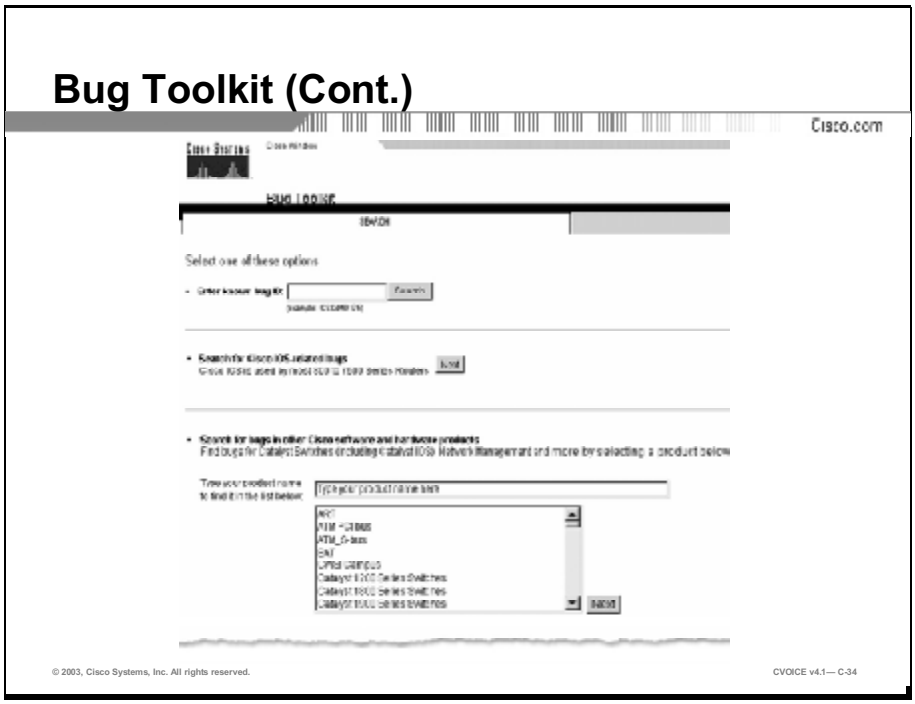


Software Advisor then lists the Cisco IOS image names, the RAM and flash memory required for each, and the product number for each, and gives a link to download the new image. Additionally, each feature has a link for more information.

The Bug Toolkit

This section explains how you can use the Bug Toolkit to search for software and hardware bugs, as well as find fixes and workarounds for them.



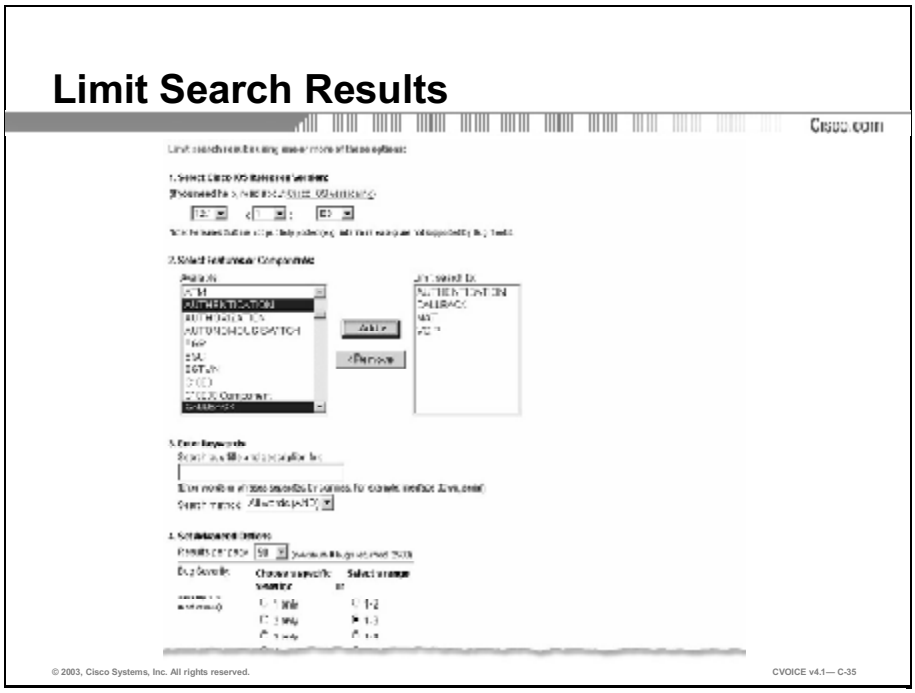


Perhaps you are considering upgrading to a new version of software or you are troubleshooting a problem with existing software. Or, you may want notification if any issues arise with your existing software. The Bug Toolkit can help you with all of these tasks. With this tool, you can search the Cisco database of known bugs for both software and hardware products. The Bug Toolkit also allows you to set up "Bug Groups," which consist of bugs that might be a concern. You then get an e-mail notification whenever the status of a bug in your group changes.

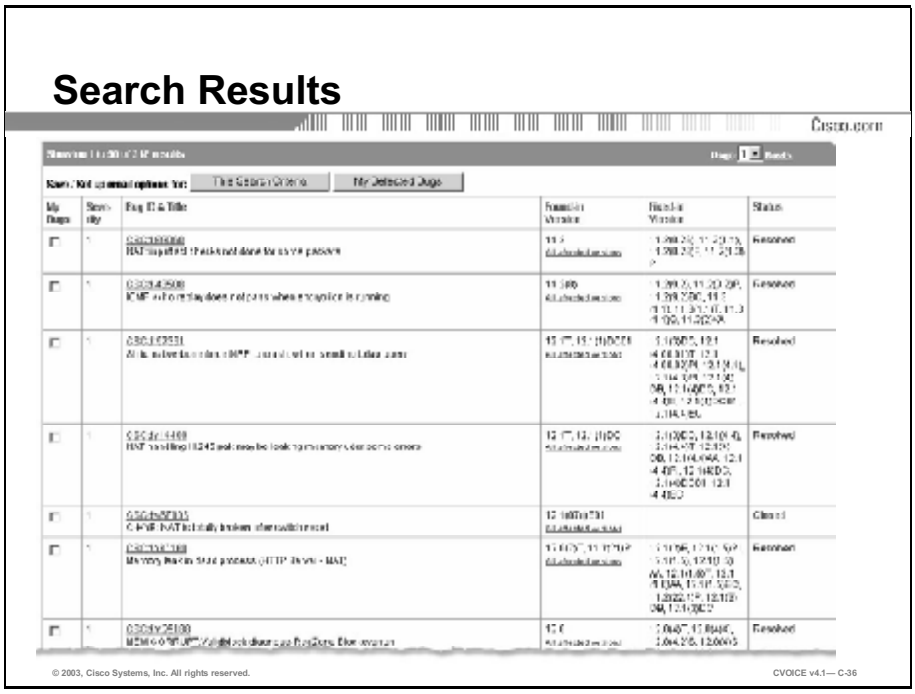
The Cisco.com Technical Assistance Center (TAC) home page contains an alphabetical listing of online tools. You can find this alphabetical listing by choosing the "Tools and Utilities" link under the "Technical Support" section of the Cisco.com home page, then select "Tools A-Z" in the menu bar on the left side of the screen. The Bug Toolkit can also be reached from the "Configuration Tools" section of the "Tools and Utilities" menu, from the Software Advisor, and from links in many other sections of Cisco.com.

Example

When researching a Cisco IOS upgrade using the Bug Toolkit, the first step is to search for Cisco IOS software related bugs by release. Next, enter the release number that you are considering. You then choose specific features or technologies to limit your search, enter a keyword or phrase, or limit the search to bugs of a certain severity level. The figure illustrates that you have chosen a Cisco IOS Version 12.1 release, are searching for any bugs within four different features, and have limited your search to bugs with a severity of 3 or worse.



Search Results

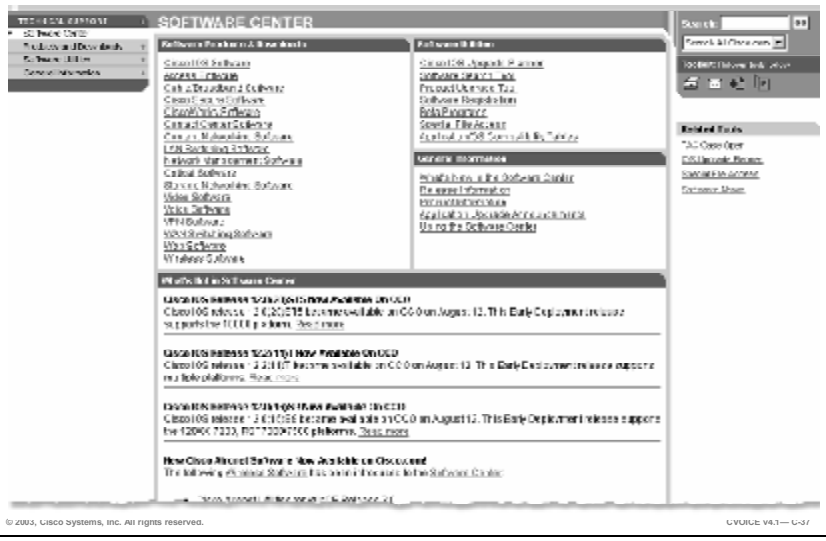


When the tool returns the search results, you see each bug ID and name, the severity of the bug, the code version, and the current state of the bug; for example, whether or not it has been resolved. For further information on a specific bug, click on the title link to view details of the issue. If you need to monitor a bug, you can choose to add it to a Bug Group. The website prompts you to create a group if you have not done so and to customize your preferences for that group.

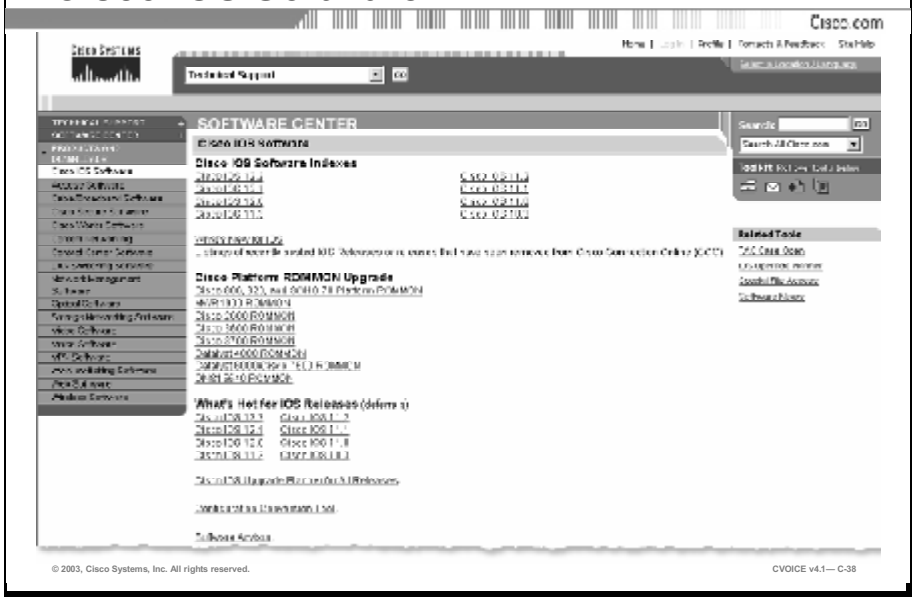
Software Center

This section explains how you can use the Software Center to obtain information about and download appropriate software releases.

Technical Assistance Center Software



Cisco IOS Software



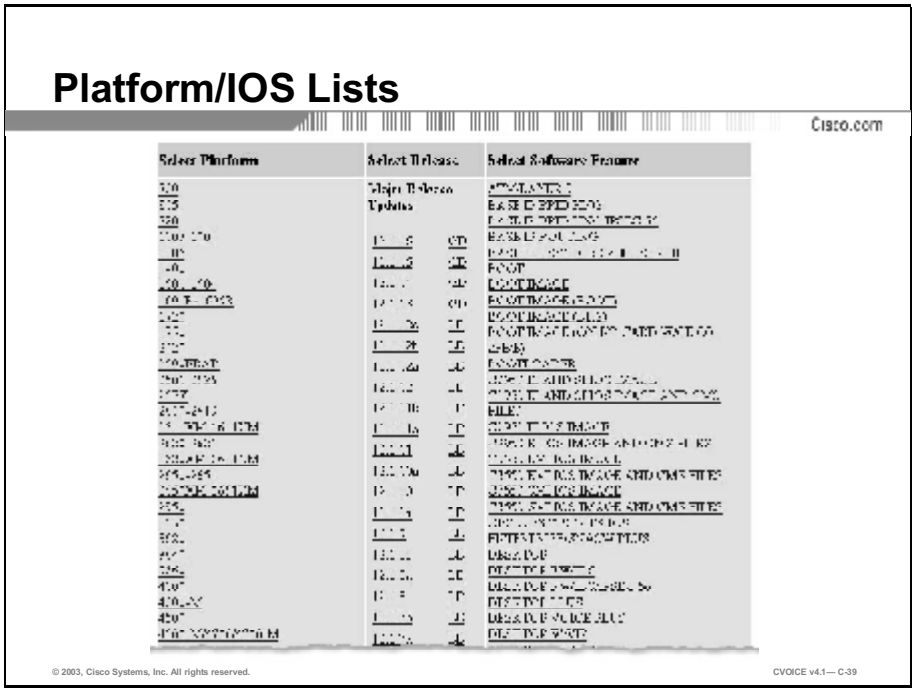
The Software Center contains the resources you need for downloading software as well as links to tools and utilities to help in your software choice. Information about downloading software is grouped by category. From the Software Center, you can reach the Cisco IOS Upgrade Planner and the Product Upgrade Tool. You can search for software and register your software. You can also reach the Software Advisor from this page.

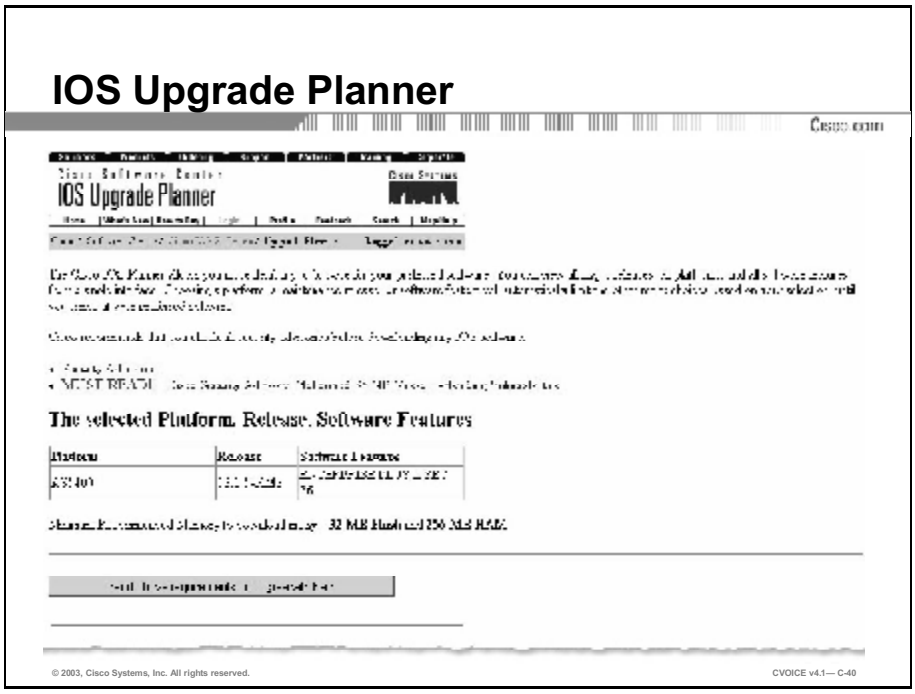
The Software Center is one of the choices in the menu that is displayed when you choose the Technical Support link on the Cisco.com home page. You can also easily reach the "Software Center" link in the Installation Tools section of the TAC home page, or the Software Advisor. Once you select the appropriate software category, you need to select the specific software release to download. Each step includes additional information and links to help you.

When you download Cisco IOS software, the Cisco IOS Upgrade Planner allows you to view all major releases, platforms, and software features from one site. Choosing a hardware platform, a release version, or a feature set will automatically redisplay a list of available options. Once you narrow your choice to one option, you can link to the download page. The download page details the RAM and flash memory that you need to run this software as well as any security advisories. You must agree to any software requirements before downloading.

Example

If you have an AS5400 and need to load Cisco IOS version 12.1, choose either the "Cisco IOS Software" category or the "Access Server" category from the main Software Center page. You need to choose Cisco IOS Software and then Cisco IOS 12.1. This allows you see the entire list of options available. Choosing the AS5400 hardware narrows the search to a list of Cisco IOS releases and feature sets that work on the AS5400. Based on your research using the Software Advisor, you will choose the Enterprise Plus IPSEC 56 feature set, release 12.1.5-XM8, which is an Early Deployment release.





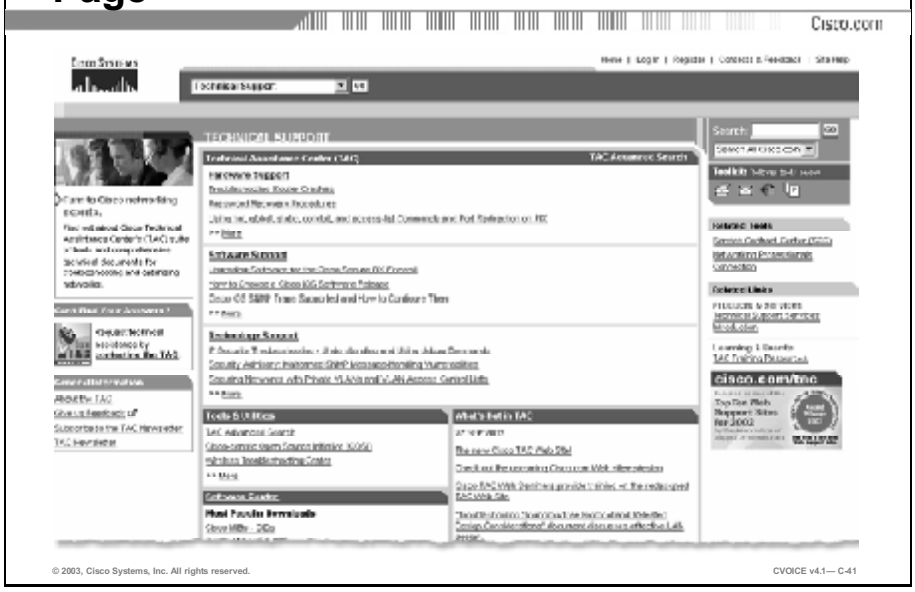
Following these steps will bring you to the download page for the chosen software. After you read and agree to the listed requirements, and read and accept the Software License Agreement on the next page, you can download the software. Make sure your equipment has the required memory and room in flash for the image.

Note	For an explanation of the various release codes, click on the *ED*, *DF*, *GD*, or *LD* link. Cisco has a white paper that explains the meaning of each of the numbers and letters in its software names. This white paper is available at: http://www.cisco.com/warp/customer/620/1.html.

Search the TAC Online

This section explains how to use the TAC portion of Cisco.com to research network issues.

Technical Assistance Center Home Page



Cisco TAC is an extremely useful resource for managing an effective network. The site is a portal to so many other online tools and so much technical content that it is important to learn to navigate around it efficiently. Cisco engineers, together with the TAC web team, developed the content to give you around-the-clock technical support. In many cases, you have access to the same online tools used by TAC engineers to resolve problems. The main TAC call centers are located in Sydney, Australia; Brussels, Belgium; and San Jose and Research Triangle Park, United States. However, TAC call centers are located around the world, so that technical assistance from a TAC engineer is available at all times. Worldwide contact information for TAC is listed, and you can request a call from the TAC support staff directly from the website.

If you are having a problem with your Cisco product, you can open a case with TAC from this site. However, by using the resources of the site you can often avoid opening a case, which saves you time and money. You can access the TAC site directly at http://www.cisco.com/tac, from the Technical Support link on Cisco.com's home page, and also from links in many other sections of Cisco.com. You need a Cisco.com login to access most of the technical material. The first thing you will notice is the task-based design; links on the TAC home page are organized by tasks that you may need to perform.

The site is divided into modules. The first three modules are Hardware Support, Software Support, and Technology Support. These three modules contain all of the technical content on the TAC website and provide an intuitive and easy way to navigate to all the technical documents and tools on the site.

Additional modules provide fast access to specific types of information on the site, such as technical support tools, software downloads, the latest TAC news, and TAC contacts. The site also features prominent links to key resources, such as the Case Open Tool, the new TAC Advanced Search, and Training Resources.

The three top modules, Hardware Support, Software Support, and Technology Support, contain all the content on the Cisco TAC website. Under the title bar of each module, you can find the three most frequently accessed documents. To access the full set of information contained in each module, you can either:

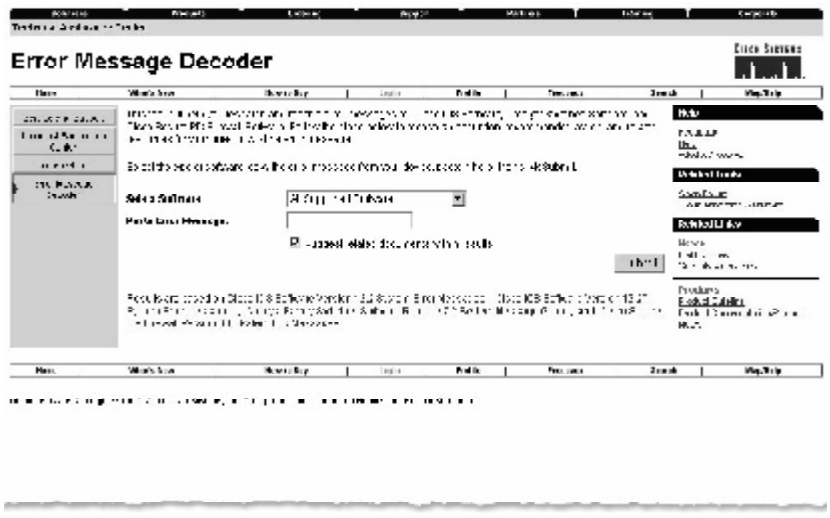
- Click on the title bar where it says Hardware Support, Software Support, or Technology Support
- Click on the word “More” that is located beneath the three most frequently accessed documents

Inside each module, you can see the full list of products or technology topics displayed alphabetically on the left-hand navigation bar. The most frequently accessed hardware, software, or technology topics are displayed in the body of the page as a featured topic. The left navigation bar tracks your movement wherever you go on the Cisco TAC website, allowing you to navigate through the site without ever losing your place.

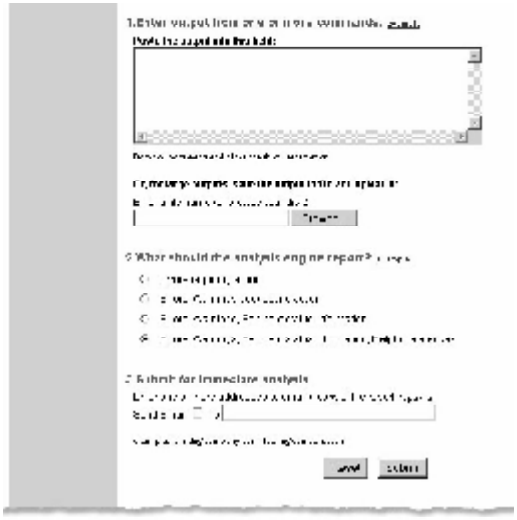
The “Tools and Utilities” module gives you direct access to all Cisco TAC tools, including the TAC Advanced Search. TAC Advanced Search is a powerful and easy-to-use tool that gives you the ability to refine your search criteria to obtain superior results. Search results only include technical support documents and resources, so you do not have to wade through unrelated content such as news postings and presales information. You can also use the TAC Advanced Search to search for all types of TAC information, including software bugs, TAC cases, and error messages.

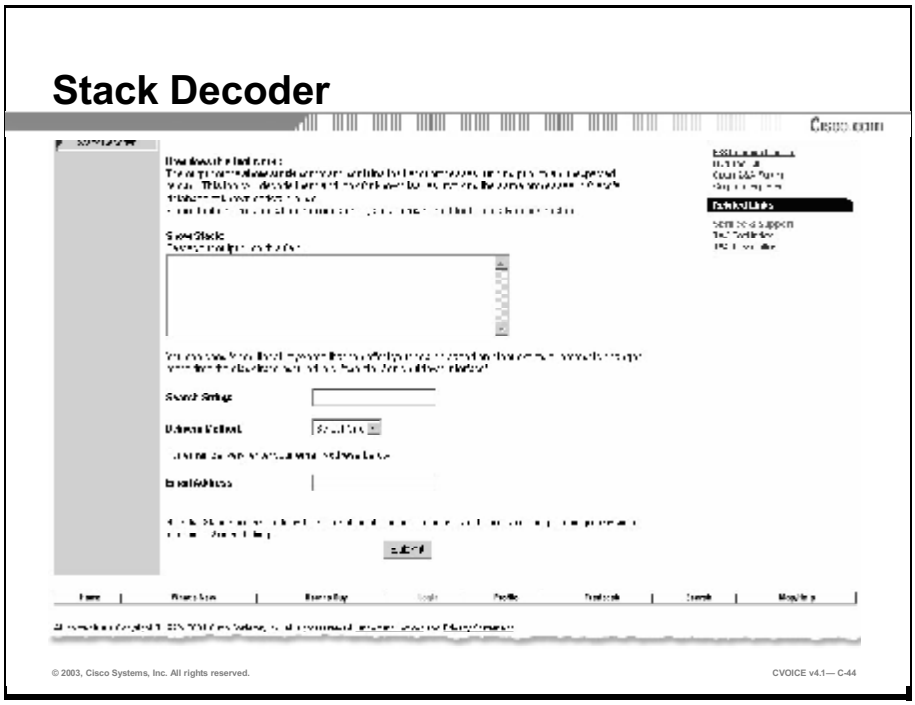
Some useful troubleshooting tools available here include the Error Message Decoder, the Output Interpreter, and the Stack Decoder, shown below. The Troubleshooting Assistance section walks you through a series of questions and answers to help you diagnose and fix problems. The questions and scenarios it contains are based on the step-by-step processes that TAC engineers follow with customers over the phone.

Error Message Decoder



Output Decoder





The “What’s Hot in TAC” module provides the latest technical support news and updates from the Cisco TAC.

The “Software Center Downloads” module offers direct access to the Cisco Software Center, where you can research and download software.

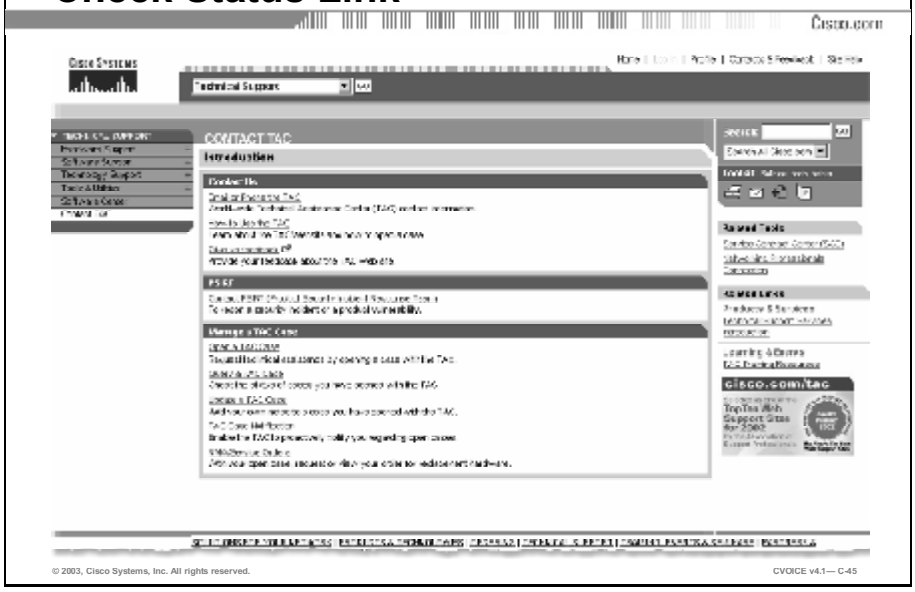
If, in spite of all these technical resources, you need to contact TAC, use the “Contact TAC” link. This is the location to check a Return Materials Authorization (RMA) status, report security incidents or product vulnerability, open a TAC case, or check its status. TAC contact information is also available here.

When you open a case using TAC, the site contains a “Recommendation Feature” link, which tries to find a solution to your problem. If possible, the Feature offers links to similar cases to help you find a solution quickly. If you still need help, you can either speak to a TAC engineer or submit your case through the website.

You can find more information using the “Related Links” and the “Related Tools” links on the right-hand side of the page. The “Networking Professionals Connection” link allows you to join discussion groups, submit questions to Cisco experts, participate in live, online technical presentations, and search the Newsgroups archives. The “Training Resources” link contains links to various seminars and learning opportunities.

“Service Contract Center” allows the management of your Cisco service contracts online. This includes viewing existing service contracts as well as pricing and ordering new contracts.

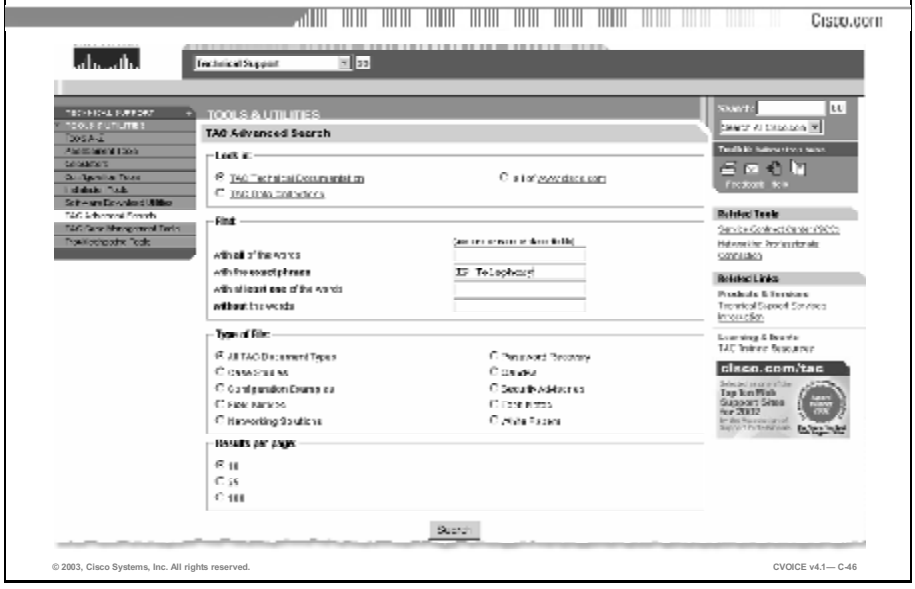
Check Status Link



Example

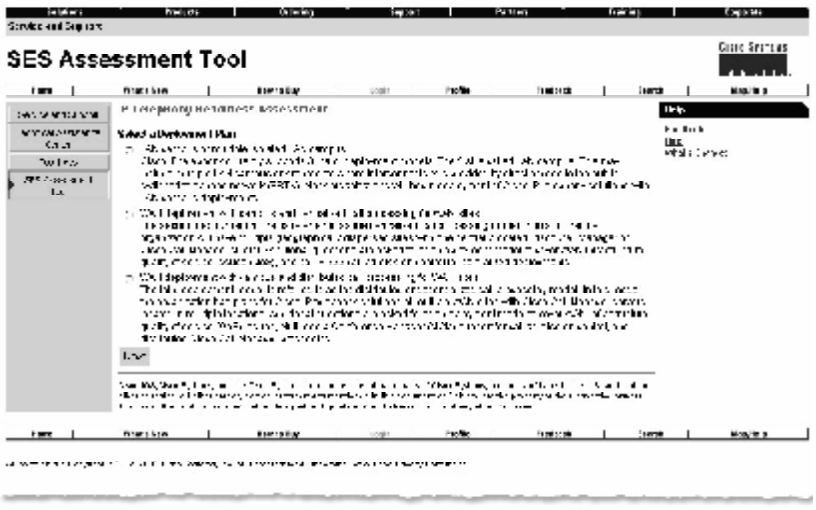
If you are designing an IP telephony solution, you may want to see what technical tips TAC offers on that subject. A search for IP telephony, using the TAC Advanced Search, yields a long list of resources, such as guides, case studies, and technical issues. By browsing the results of your search, you can take a closer look at items of interest. For example, there is an IP Telephony Readiness Assessment that might help you.

Technical Assistance Center Search



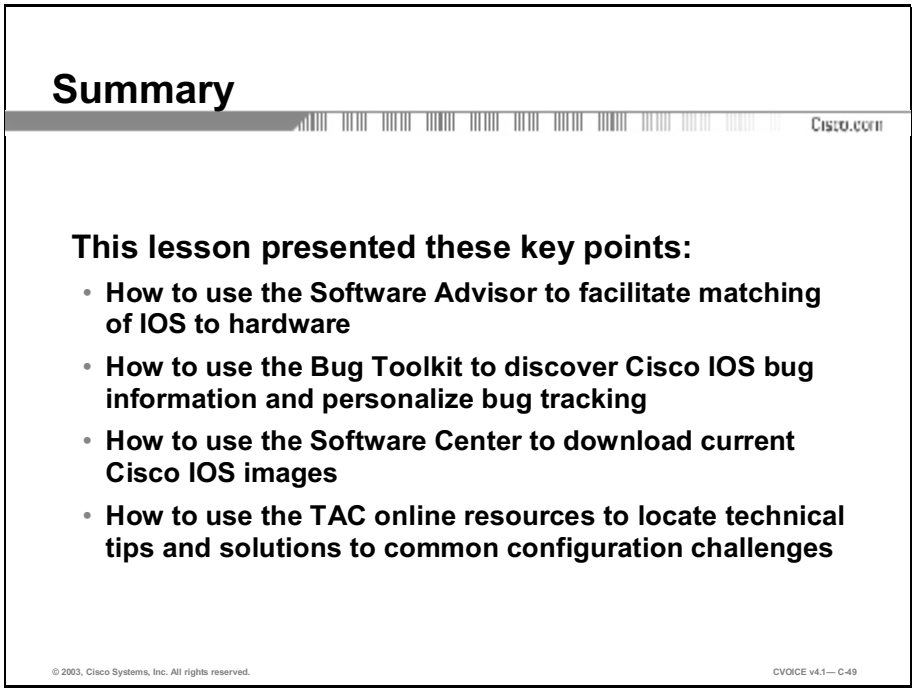
Search Results

Assessment Tool



Summary

This section summarizes the key points discussed in this lesson.



Next Steps

After completing this lesson, go to:

- Assessment (Quiz): Specialized Tools

References

For additional information, refer to these resources:

- http://www.cisco.com/tac

Quiz: Specialized Tools

Complete the quiz to assess what you have learned in this lesson.

Objectives

This quiz tests your knowledge on how to:

- Use the Software Advisor
- Use the Bug Toolkit
- Use the Software Center
- Search TAC Online

Instructions

Answer these questions.

Q1) Match the tool to the task. You may use each tool more than once.

A) Software Advisor

B) Bug Toolkit

C) Software Center

D) TAC Online

_____ 1. Download Cisco IOS software

_____ 2. Research known bugs in a specific software version

_____ 3. Submit a technical support case to TAC

_____ 4. Compare versions of the Cisco IOS or CatOS software

_____ 5. Register software

_____ 6. Research known bugs in a specific hardware product

_____ 7. Search for an Cisco IOS version based on features

_____ 8. Submit a question to a Cisco expert

_____ 9. Set up a “Bug Group”

_____ 10. Find solutions to the most frequent issues with a specific technology

Scoring

You have successfully completed the quiz for this lesson when you earn a score of 80 percent or better.

D

Lab Pull-Out Resource

Lab Resource

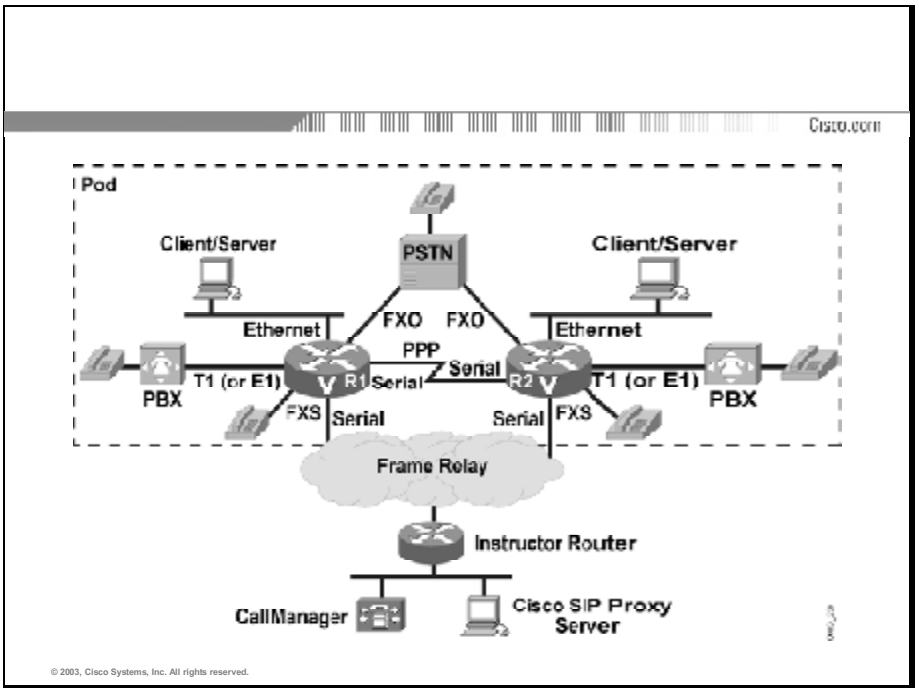


Table 1: IP Address Assignment

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

Table 2: Hostname Table

Pod Number	Router	Hostname
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 the following 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.

Table 3: Classroom Dial Plan

Pod Number		1	2	3	4	5	6
R1		1101 1102	2101 2102	3101 3102	4101 4102	5101 5102	6101 6102
PBX1		1151	2151	3151	4151	5151	6151
R2		1201 1202	2201 2202	3201 3202	4201 4202	5201 5202	6201 6202
PBX2		1251	2251	3251	4251	5251	6251
PSTN	Port 1 Port 2 Port 3	555-1001 555-1002 555-1003	555-2001 555-2002 555-2003	555-3001 555-3002 555-3003	555-4001 555-4002 555-4003	555-5001 555-5002 555-5003	555-6001 555-6002 555-6003

