CIPT1

Cisco Voice over IP

Volume 1

Version 6.0

Student Guide

Editorial, Production, and Web Services: 02.15.08

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

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

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

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

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

Students, this letter describes important course evaluation access information!

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

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

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

Sincerely,

Cisco Systems Learning

Table of Contents

Volume 1

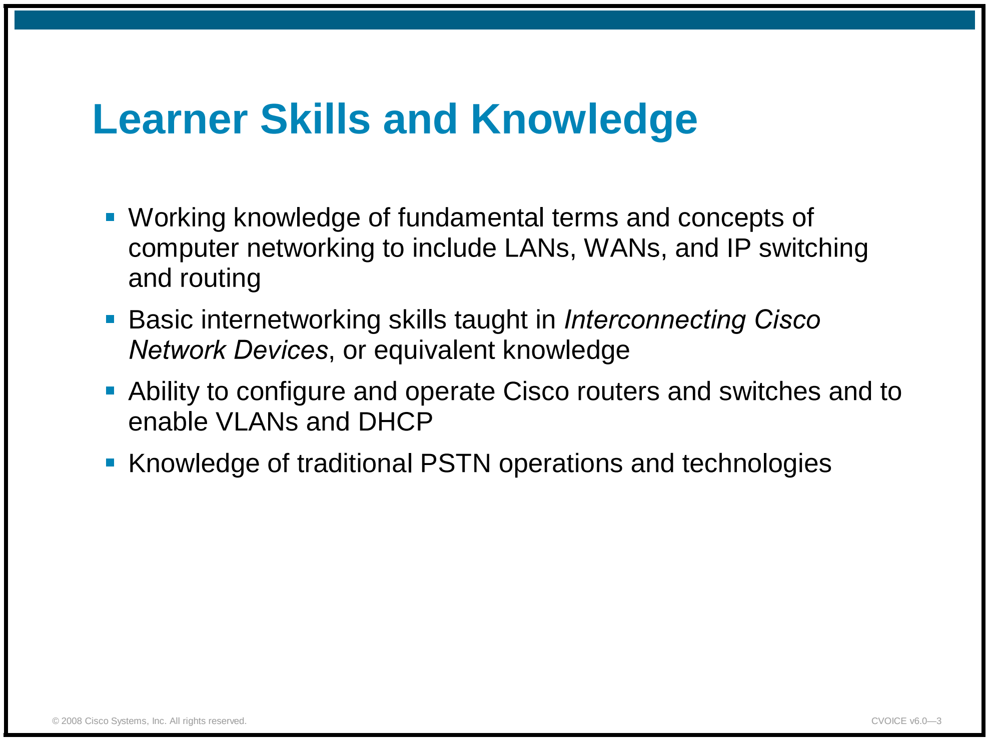
Course Introduction

Overview

Cisco Voice over IP (CVOICE) v6.0 provides an understanding of converged voice and data networks and the challenges the various network technologies face. The course also provides network administrators and network engineers with the knowledge and skills that are required to integrate gateways and gatekeepers into an enterprise VoIP network. This course is one of several courses in the Cisco CCVP™ track that addresses design, planning, and deployment practices and provides comprehensive hands-on experience in configuration and deployment of VoIP networks.

Learner Skills and Knowledge

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



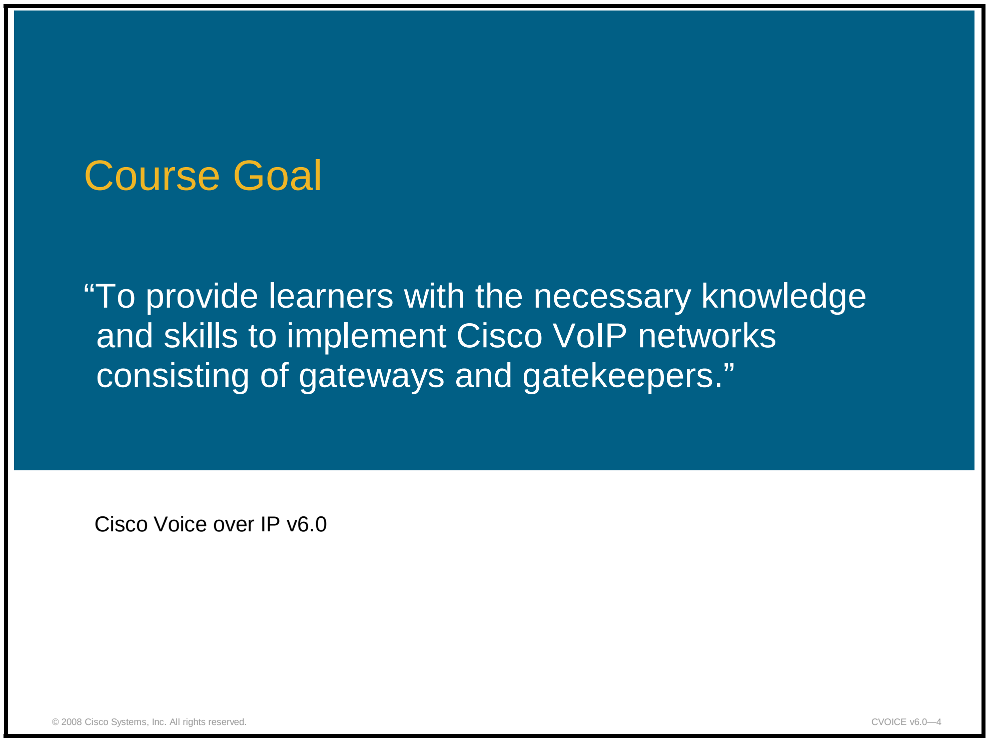
Learner Skills and Knowledge

- Working knowledge of fundamental terms and concepts of computer networking to include LANs, WANs, and IP switching and routing
- Basic internetworking skills taught in *Interconnecting Cisco Network Devices*, or equivalent knowledge
- Ability to configure and operate Cisco routers and switches and to enable VLANs and DHCP
- Knowledge of traditional PSTN operations and technologies

CVOICE v6.0—3

Course Goal and Objectives

This topic describes the course goal and objectives.



Course Goal

"To provide learners with the necessary knowledge and skills to implement Cisco VoIP networks consisting of gateways and gatekeepers."

Cisco Voice over IP v6.0

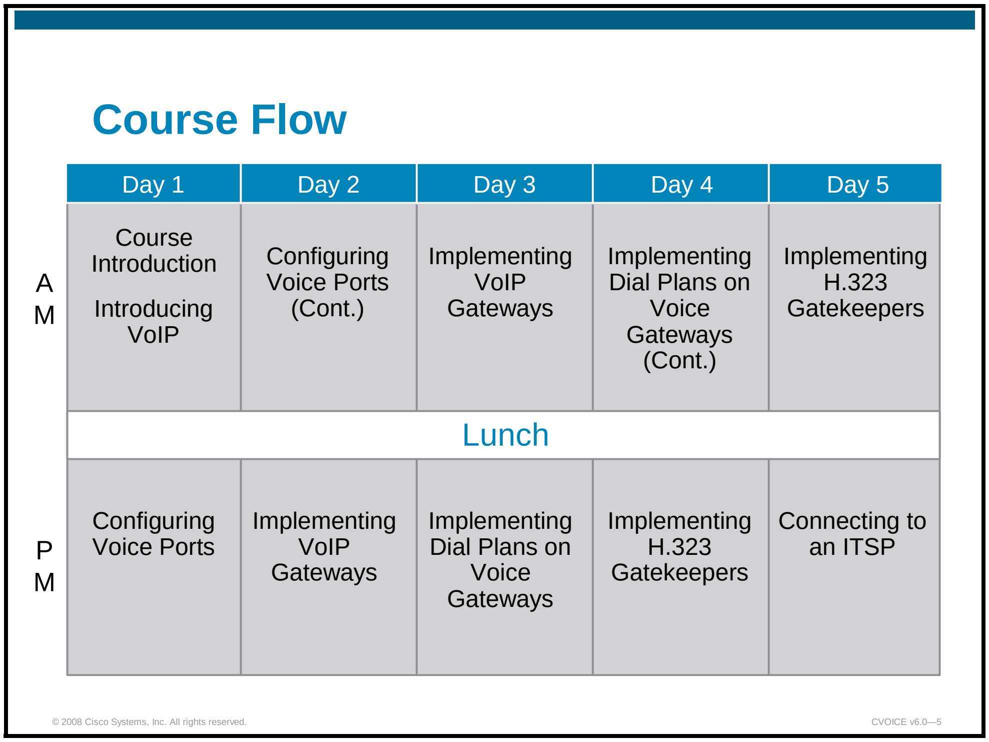
© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—4

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

- Describe VoIP, voice gateways, special requirements for VoIP calls, codecs and codec complexity, and how DSPs are used as media resources on a voice gateway
- Configure gateway interconnections to support VoIP and PSTN calls and to integrate with a PSTN and PBX
- Describe the basic signaling protocols that are used on voice gateways and configure a gateway to support calls using the various signaling protocols
- Define a dial plan, describe the purpose of each dial plan component, and implement a dial plan on a voice gateway
- Implement gatekeepers and directory gatekeepers, and identify redundancy options for gatekeepers
- Implement a Cisco UBE gateway to connect to an Internet telephony service provider

Course Flow

This topic presents the suggested flow of the course materials.



Course Flow

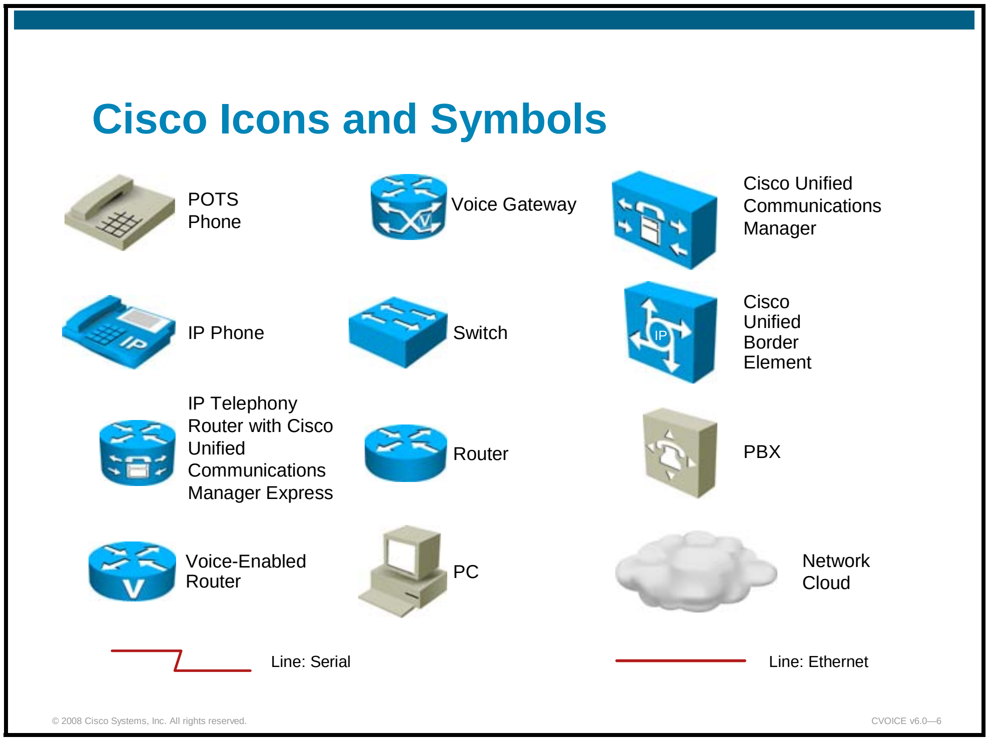
	Day 1	Day 2	Day 3	Day 4	Day 5
A M	Course Introduction Introducing VoIP	Configuring Voice Ports (Cont.)	Implementing VoIP Gateways	Implementing Dial Plans on Voice Gateways (Cont.)	Implementing H.323 Gatekeepers
	Lunch				
P M	Configuring Voice Ports	Implementing VoIP Gateways	Implementing Dial Plans on Voice Gateways	Implementing H.323 Gatekeepers	Connecting to an ITSP

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

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

Additional References

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



Cisco Icons and Symbols

POTS Phone

Voice Gateway

Cisco Unified Communications Manager

IP Phone

Switch

Cisco Unified Border Element

IP Telephony Router with Cisco Unified Communications Manager Express

Router

PBX

Voice-Enabled Router

PC

Network Cloud

Line: Serial

Line: Ethernet

Cisco Glossary of Terms

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

Your Training Curriculum

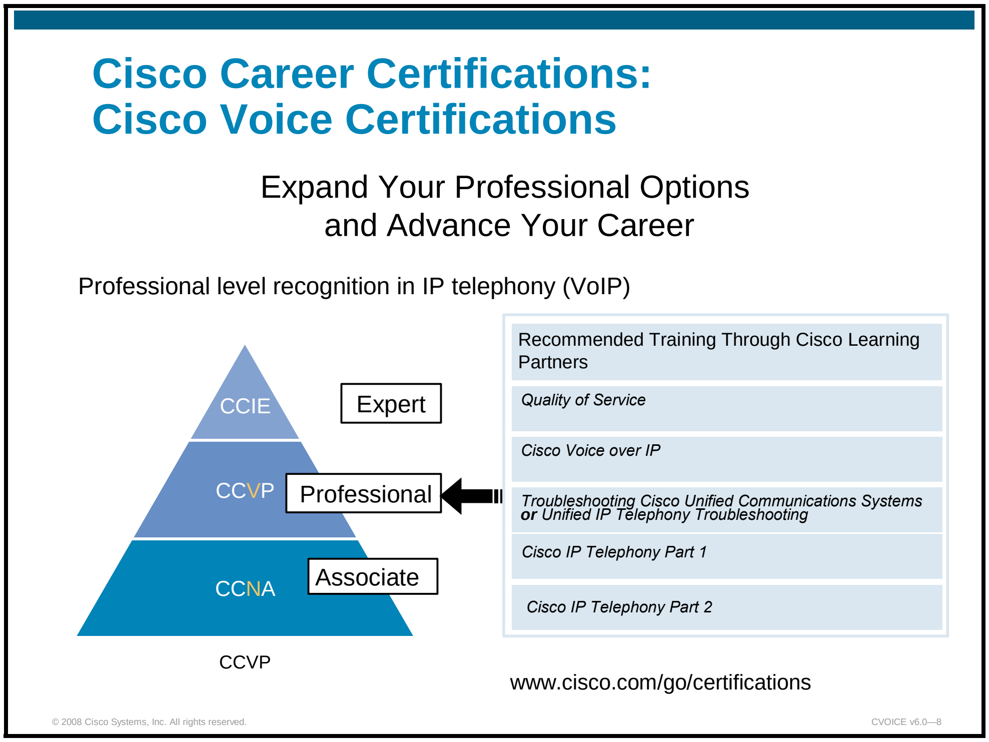
This topic presents the training curriculum for this course.

Cisco Career Certifications

Cisco Certifications

www.cisco.com/go/certifications

You are encouraged to join the Cisco Certification Community, a discussion forum open to anyone holding a valid Cisco Career Certification (such as Cisco CCIE®, CCNA®, CCDA®, CCNP®, CCDP®, CCIP®, CCVP™, or CCSP™). It provides a gathering place for Cisco certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit www.cisco.com/go/certifications.



Cisco Career Certifications: Cisco Voice Certifications

Expand Your Professional Options
and Advance Your Career

Professional level recognition in IP telephony (VoIP)

CCIE — Expert

CCVP — Professional

CCNA — Associate

CCVP

Recommended Training Through Cisco Learning Partners
Quality of Service
Cisco Voice over IP
Troubleshooting Cisco Unified Communications Systems ***or*** *Unified IP Telephony Troubleshooting*
Cisco IP Telephony Part 1
Cisco IP Telephony Part 2

www.cisco.com/go/certifications

CVOICE v6.0—8

Module 1

Introduction to VoIP

Overview

VoIP enables a voice-enabled router to carry voice traffic, such as telephone calls and faxes, over an IP network. This module introduces the fundamentals of VoIP, discussing components and available voice-signaling protocols of a VoIP network, as well as service considerations when you are integrating a VoIP component into existing data network. The module describes various types of voice gateways and how to use gateways in different IP telephony environments. Special requirements for VoIP calls are also discussed. In addition, this module explains codecs and digital signal processors (DSPs) and their impact on VoIP implementations.

Module Objectives

Upon completing this module, you will be able to describe VoIP, voice gateways, requirements for VoIP calls, codecs and codec complexity, and how DSPs are used as media resources on a voice gateway. This ability includes being able to meet these objectives:

- Describe VoIP, the components of a VoIP network, the protocols used, and the service considerations of integrating VoIP into an existing data network
- Describe the various types of voice gateways and how to use gateways in different IP telephony environments
- Describe special requirements for VoIP calls, including the need for QoS and fax relay, modem relay, and DTMF support
- Describe various codecs, how to configure codec complexity, and how DSPs are used as media resources

Lesson 1

Introducing VoIP

Overview

VoIP is also known as IP telephony or broadband telephony. It routes voice conversations over IP-based networks including the Internet. VoIP has made it possible for businesses to realize cost savings by utilizing their existing IP network to carry voice and data, especially where businesses have underutilized network capacity that can carry VoIP at no additional cost. This lesson introduces VoIP, the components required in VoIP networks, currently available VoIP signaling protocols, VoIP service issues, and media transmission protocols.

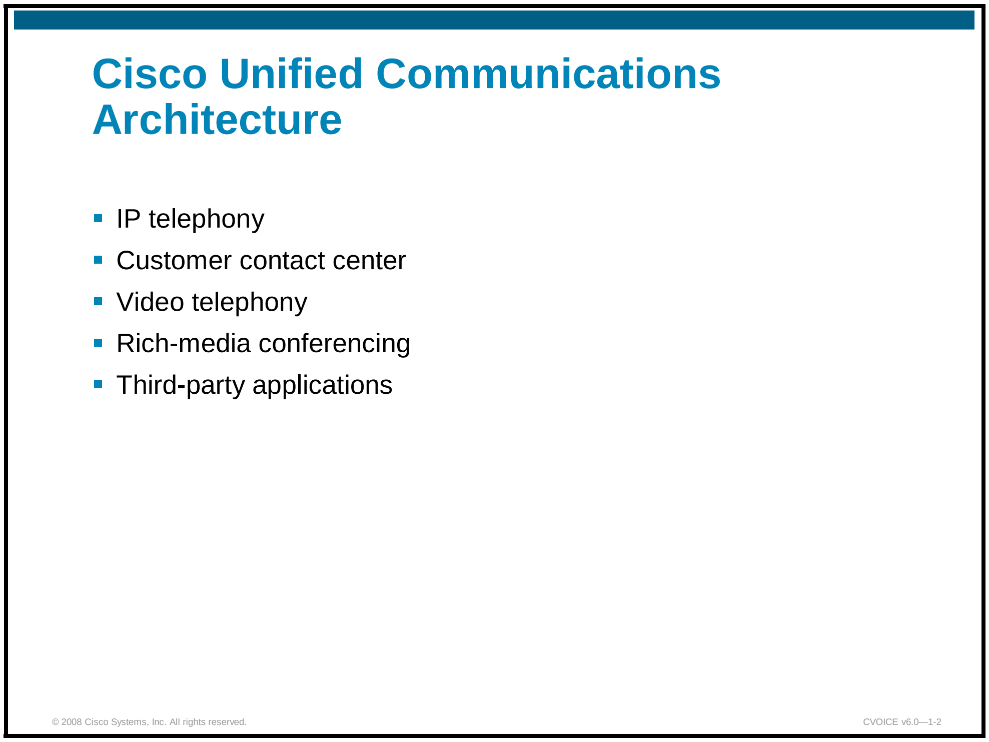
Objectives

Upon completing this lesson, you will be able to describe the different types of voice gateways, including their functions, protocols, and uses. This will include being able to meet these objectives:

- Describe the components of the Cisco Unified Communications architecture
- Describe VoIP and the basic components of a VoIP network
- Describe the major VoIP signaling protocols
- Describe the differences between the gateway signaling protocols
- Describe issues that can affect voice service in the IP network
- Describe characteristics of the protocols used for media transmission

Cisco Unified Communications Architecture

This topic describes the components of the Cisco Unified Communications architecture.



Cisco Unified Communications Architecture

- IP telephony
- Customer contact center
- Video telephony
- Rich-media conferencing
- Third-party applications

CVOICE v6.0—1-2

The Cisco Unified Communications system fully integrates communications by enabling data, voice, and video to be transmitted over a single network infrastructure using standards-based IP. Leveraging the framework provided by Cisco IP hardware and software products, the Cisco Unified Communications system has the capability to address current and emerging communications needs in the enterprise environment. The Cisco Unified Communications family of products is designed to optimize feature functionality, reduce configuration and maintenance requirements, and provide interoperability with a wide variety of other applications. The Cisco Unified Communications system provides and maintains a high level of availability, quality of service (QoS), and security for the network.

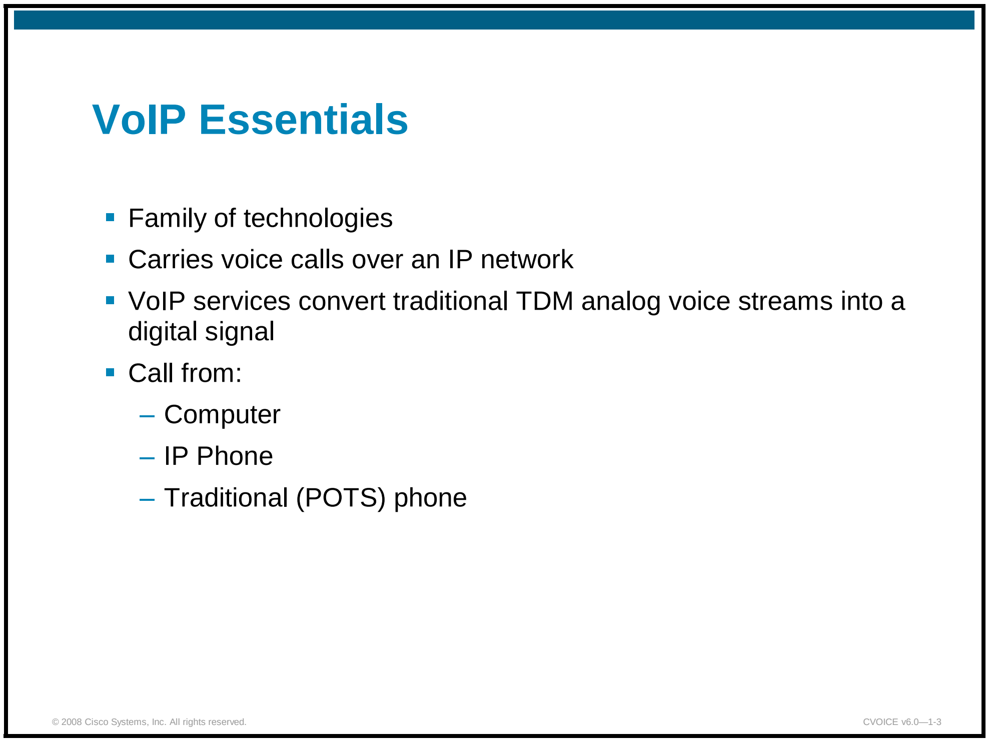
The Cisco Unified Communications system incorporates and integrates the following communications technologies:

- **IP telephony:** IP telephony refers to technology that transmits voice communications over a network using IP standards. Cisco Unified Communications includes hardware and software products such as call-processing agents, IP phones (both wired and wireless), voice-messaging systems, video devices, and many special applications.
- **Customer contact center:** Cisco IP Contact Center products combine strategy with architecture to enable efficient and effective customer communications across a globally capable network. This strategy allows organizations to draw from a broader range of resources to service customers. These resources include access to a large pool of agents and multiple channels of communication as well as customer self-help tools.
- **Video telephony:** Cisco Unified Video Advantage products enable real-time video communications and collaboration using the same IP network and call-processing agent as Cisco Unified Communications. With Cisco Unified Video Advantage, making a video call is just as easy as dialing a phone number.

- **Rich-media conferencing:** Cisco Conference Connection and Cisco Unified MeetingPlace enhance the virtual meeting environment with an integrated set of IP-based tools for voice, video, and web conferencing.
- **Third-party applications:** Cisco works with cutting-edge companies to provide a broad selection of third-party IP communications applications and products. These third-party applications help businesses focus on critical needs such as messaging, customer care, and workforce optimization.

VoIP Essentials

This topic describes VoIP and the basic components of a VoIP network.



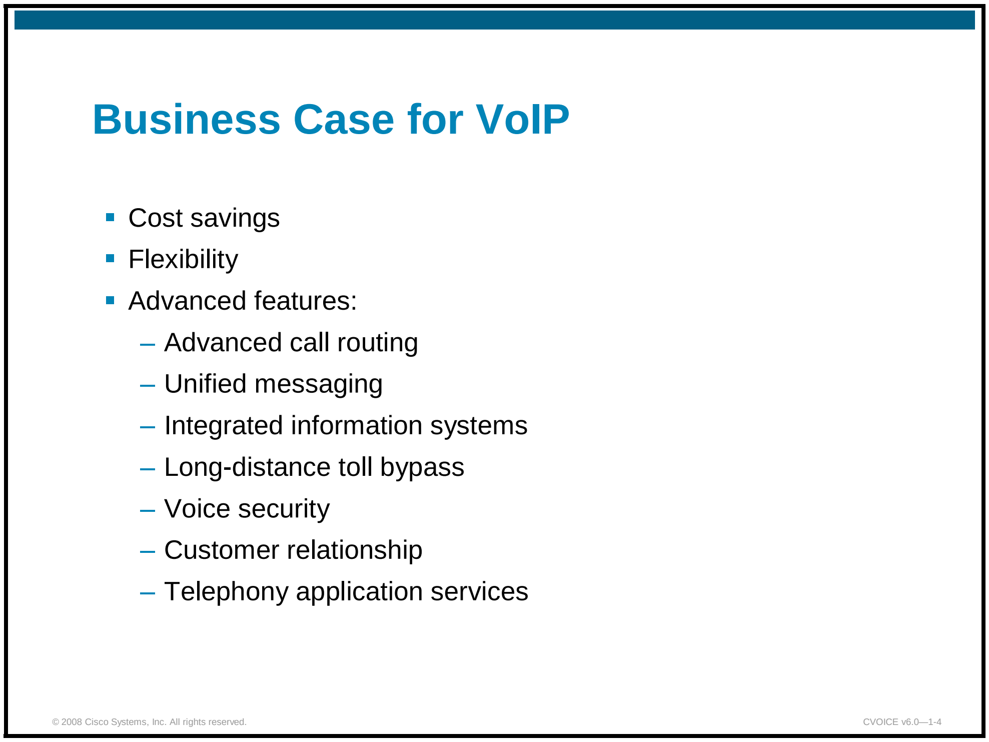
VoIP Essentials

- Family of technologies
- Carries voice calls over an IP network
- VoIP services convert traditional TDM analog voice streams into a digital signal
- Call from:
  - Computer
  - IP Phone
  - Traditional (POTS) phone

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-3

VoIP is the family of technologies that allow IP networks to be used for voice applications such as telephony, voice instant messaging, and teleconferencing. VoIP defines a way to carry voice calls over an IP network, including how voice streams are digitized and packetized. IP telephony utilizes VoIP standards to create a telephony system where higher-level features, such as advanced call routing, voice mail, contact centers, and so on, can be utilized.

VoIP services convert your voice into a digital signal that travels over the Internet. If you are calling a traditional phone number, the signal is converted to a traditional telephone signal before it reaches the destination. VoIP allows you to make a call directly from a computer, a special VoIP phone, or a traditional phone connected to a special adapter. In addition, wireless “hot spots” in locations such as airports, parks, and cafes that allow you to connect to the Internet may enable you to use VoIP service.



Business Case for VoIP

- Cost savings
- Flexibility
- Advanced features:
  - Advanced call routing
  - Unified messaging
  - Integrated information systems
  - Long-distance toll bypass
  - Voice security
  - Customer relationship
  - Telephony application services

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-4

Business Case

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

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

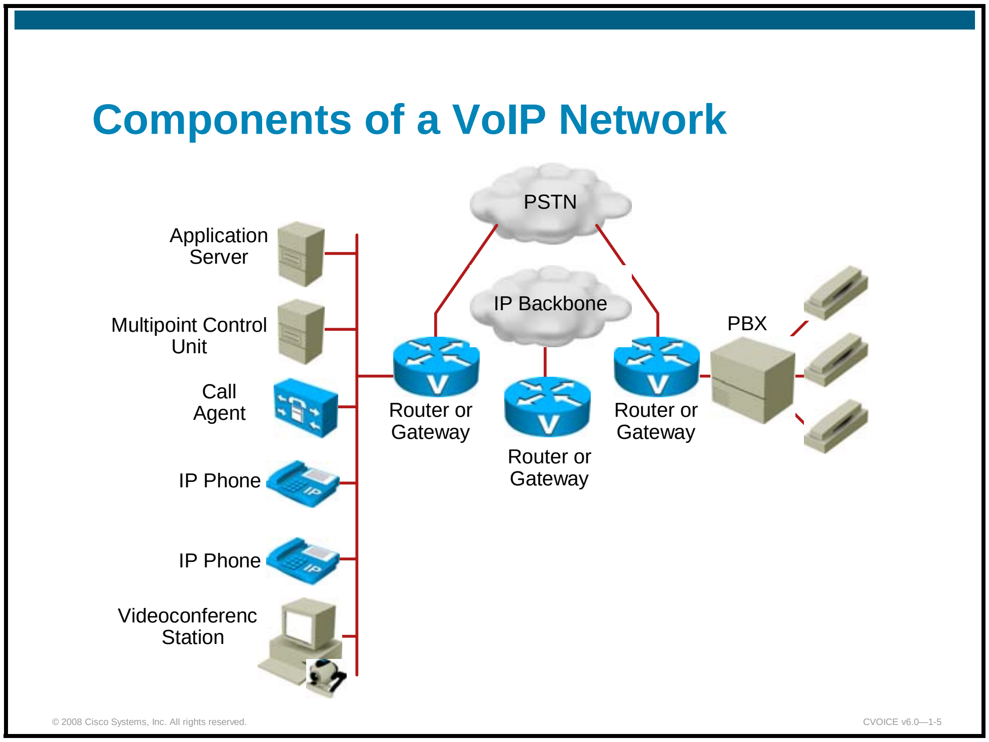
- **Cost savings:** Traditional time-division multiplexing (TDM), which is used in the public switched telephone network (PSTN) environment, dedicates 64 kb/s of bandwidth per voice channel. This approach results in unused bandwidth when there is no voice traffic. VoIP shares bandwidth across multiple logical connections, which makes more efficient use of the bandwidth and thereby reducing bandwidth requirements. A substantial amount of equipment is needed to combine 64-kb/s channels into high-speed links for transport across the network. Packet telephony uses statistical analysis to multiplex voice traffic alongside data traffic. This consolidation results in substantial savings on capital equipment and operations costs.
- **Flexibility:** The sophisticated functionality of IP networks allows organizations to be flexible in the types of applications and services that they provide to their customers and users. Service providers can easily segment customers. This segmentation helps them to provide different applications, custom services, and rates depending on the traffic volume needs and other customer-specific factors.
- **Advanced features:** Here are some examples of the advanced features provided by current VoIP applications.
  - **Advanced call routing:** When multiple paths exist to connect a call to its destination, some of these paths may be preferred over others based on cost, distance, quality, partner handoffs, traffic load, or various other considerations.

Least-cost routing and time-of-day routing are two examples of advanced call routing that can be implemented to determine the best possible route for each call.

- **Unified messaging:** Unified messaging improves communications and productivity. It provides a single user interface for messages that have been delivered over a variety of media. For example, users can read their e-mail, hear their voice mail, and view fax messages by accessing a single inbox.
- **Integrated information systems:** Organizations use VoIP to affect business process transformation. These processes include centralized call control, geographically dispersed virtual contact centers, and access to resources and self-help tools.
- **Long-distance toll bypass:** Long-distance toll bypass is an attractive solution for organizations that place a significant number of calls between sites that are charged traditional long-distance fees. In this case, it may be more cost-effective to use VoIP to place those calls across the IP network. If the IP WAN becomes congested, calls can overflow into the PSTN, ensuring that there is no degradation in voice quality.
- **Voice security:** There are mechanisms in the IP network that allow the administrator to ensure that IP conversations are secure. Encryption of sensitive signaling header fields and message bodies protect the packets in case of unauthorized packet interception.
- **Customer relationships:** The ability to provide customer support through multiple media such as telephone, chat, and e-mail, builds solid customer satisfaction and loyalty. A pervasive IP network allows organizations to provide contact center agents with consolidated and up-to-date customer records along with the related customer communication. Access to this information allows quick problem solving, which, in turn, builds strong customer relationships.
- **Telephony application services:** Extensible Markup Language (XML) services on Cisco Unified IP phones give users another way to perform or access more business applications. Some examples of XML-based services on IP phones are user stock quotes, inventory checks, direct-dial directory, announcements, and advertisements. The IP phones are equipped with a pixel-based display that can show full graphics instead of just text on the window. The pixel-based display capabilities allow you to use sophisticated graphical presentations for applications on Cisco IP phones and make them available at any desktop, counter, or location.

Components of a VoIP Network

This subtopic introduces the basic components of a VoIP network.



Components of a VoIP Network

CVOICE v6.0—1-5

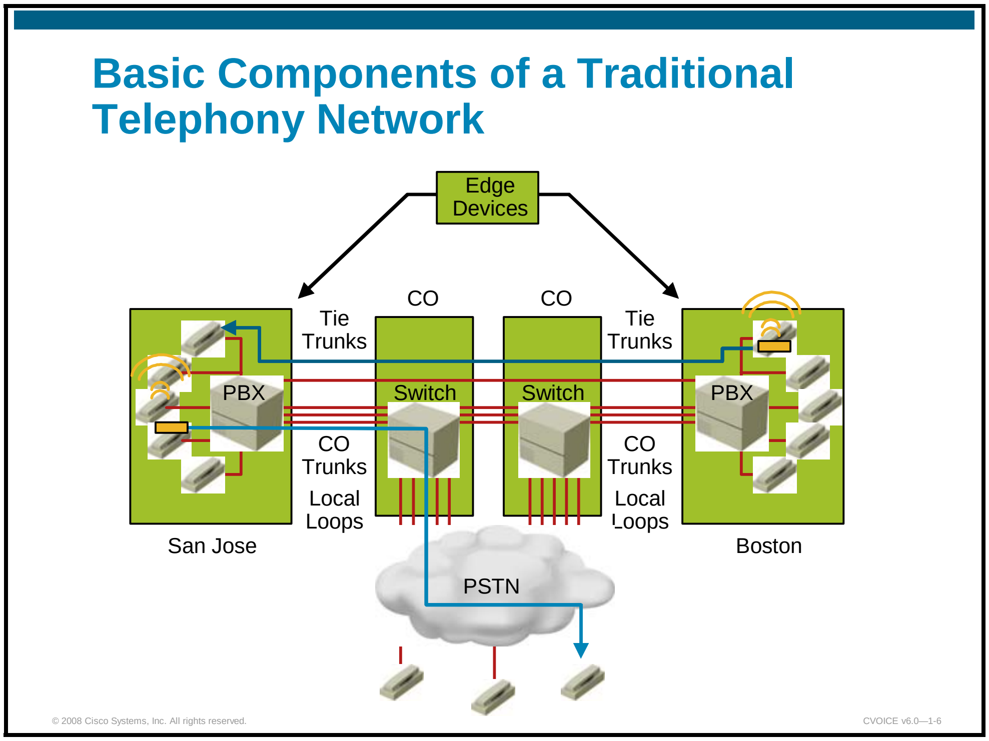
The figure depicts the basic components of a packet voice network:

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

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

VoIP Functions

This subtopic describes signaling, database services, bearer control, and coder-decoder (codec) functions of VoIP, and compares them to similar functions of a PSTN.



Basic Components of a Traditional Telephony Network

CVOICE v6.0—1-6

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

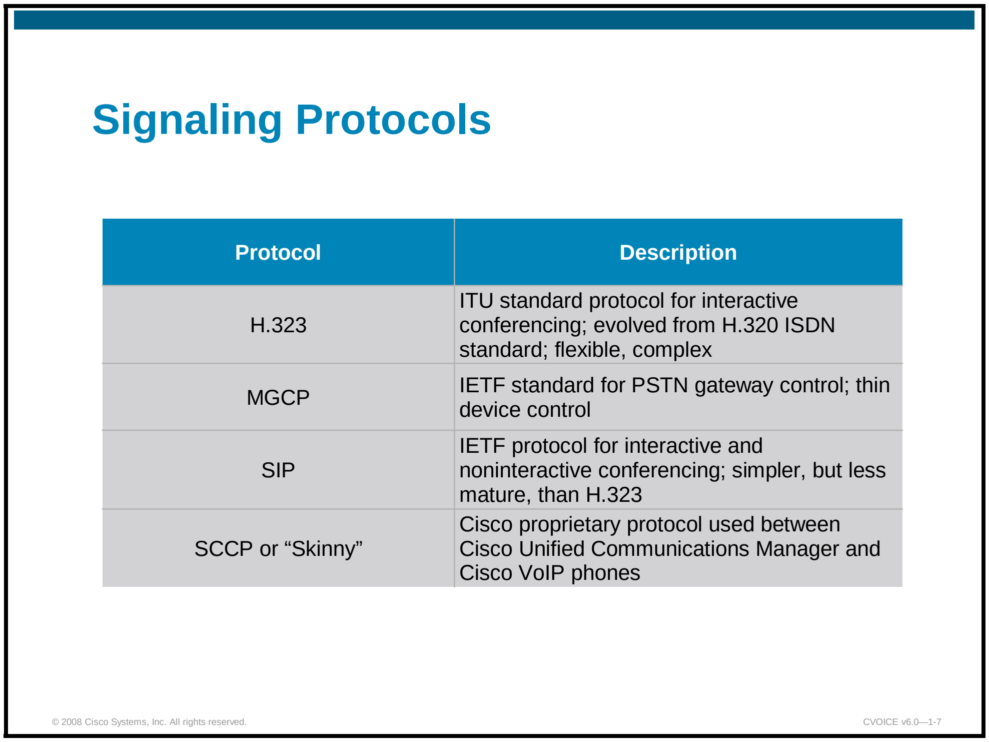
Required VoIP functionality includes these functions:

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

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

VoIP Signaling Protocols

This topic describes the major VoIP signaling protocols.



Signaling Protocols

Protocol	Description
H.323	ITU standard protocol for interactive conferencing; evolved from H.320 ISDN standard; flexible, complex
MGCP	IETF standard for PSTN gateway control; thin device control
SIP	IETF protocol for interactive and noninteractive conferencing; simpler, but less mature, than H.323
SCCP or “Skinny”	Cisco proprietary protocol used between Cisco Unified Communications Manager and Cisco VoIP phones

CVOICE v6.0—1-7

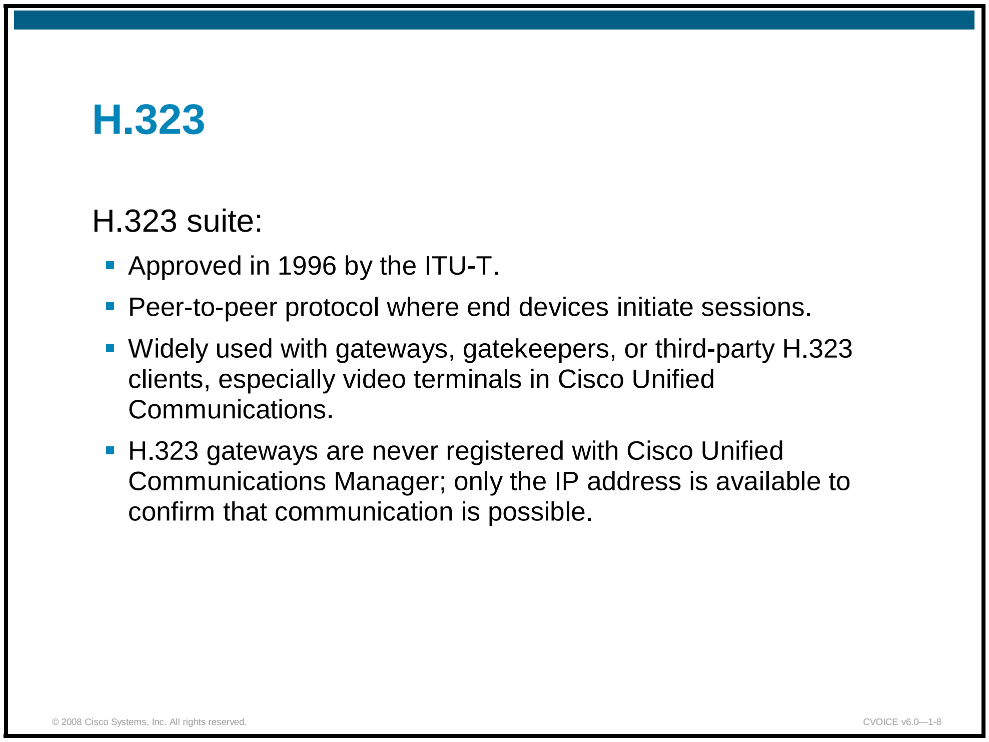
VoIP uses several control and call signaling protocols.

- **H.323:** H.323 is a standard that specifies the components, protocols, and procedures that provide multimedia communication services—real-time audio, video, and data communications—over packet networks, including IP networks. H.323 is part of a family of ITU-T recommendations called H.32x that provides multimedia communication services over a variety of networks. It is actually an umbrella of standards that define all aspects of synchronized voice, video, and data transmission. It also defines end-to-end call signaling.
- **MGCP:** MGCP is a method for PSTN gateway control or thin device control. Specified in RFC 2705, MGCP defines a protocol that controls VoIP gateways that are connected to external call control devices, referred to as call agents. MGCP provides the signaling capability for less expensive edge devices, such as gateways, that may not have a full voice-signaling protocol such as H.323 implemented. For example, any time an event such as off hook occurs at the voice port of a gateway, the voice port reports that event to the call agent. The call agent then signals that device to provide a service, such as dial-tone signaling.
- **SIP:** SIP is a detailed protocol that specifies the commands and responses to set up and tear down calls. SIP also details features such as security, proxy, and transport control protocol (TCP or User Datagram Protocol [UDP]) services. SIP and its partner protocols, Session Announcement Protocol (SAP) and Session Description Protocol (SDP), provide announcements and information about multicast sessions to users on a network. SIP defines end-to-end call signaling between devices. SIP is a text-based protocol that borrows many elements of HTTP, using the same transaction request and response model and similar header and response codes. It also adopts a modified form of the URL addressing scheme that is used within e-mail that is based on Simple Mail Transfer Protocol (SMTP).

- **SCCP:** SCCP is a Cisco proprietary protocol used between Cisco Unified Communications Manager and Cisco VoIP phones. The end stations (telephones) that use SCCP are called Skinny clients, which consume less processing overhead. The client communicates with the Cisco Unified Communications Manager using connection-oriented (TCP/IP-based) communication to establish a call with another H.323-compliant end station.

H.323 Suite

This subtopic covers the H.323 family of protocols.



H.323

H.323 suite:

- Approved in 1996 by the ITU-T.
- Peer-to-peer protocol where end devices initiate sessions.
- Widely used with gateways, gatekeepers, or third-party H.323 clients, especially video terminals in Cisco Unified Communications.
- H.323 gateways are never registered with Cisco Unified Communications Manager; only the IP address is available to confirm that communication is possible.

H.323 is a suite of protocols defined by the ITU for multimedia conferences over LANs. The H.323 protocol was designed by the ITU-T and initially approved in February 1996. It was developed as a protocol that provides IP networks with traditional telephony functionality. Today, H.323 is the most widely deployed standards-based voice and videoconferencing standard for packet-switched networks.

The protocols specified by H.323 include the following:

- **H.225 call signaling:** H.225 call signaling is used to establish a connection between two H.323 endpoints. This connection is achieved by exchanging H.225 protocol messages on the call-signaling channel. The call-signaling channel is opened between two H.323 endpoints or between an endpoint and the gatekeeper.
- **H.225 Registration, Admission, and Status:** Registration, Admission, and Status (RAS) is the protocol between endpoints (terminals and gateways) and gatekeepers. The RAS is used to perform registration, admission control, bandwidth changes, and status and disengage procedures between endpoints and gatekeepers. A RAS channel is used to exchange RAS messages. This signaling channel is opened between an endpoint and a gatekeeper prior to the establishment of any other channels.
- **H.245 control signaling:** H.245 control signaling is used to exchange end-to-end control messages governing the operation of the H.323 endpoint. These control messages carry information related to the following:
  - Capabilities exchange
  - Opening and closing of logical channels used to carry media streams
  - Flow-control messages
  - General commands and indications

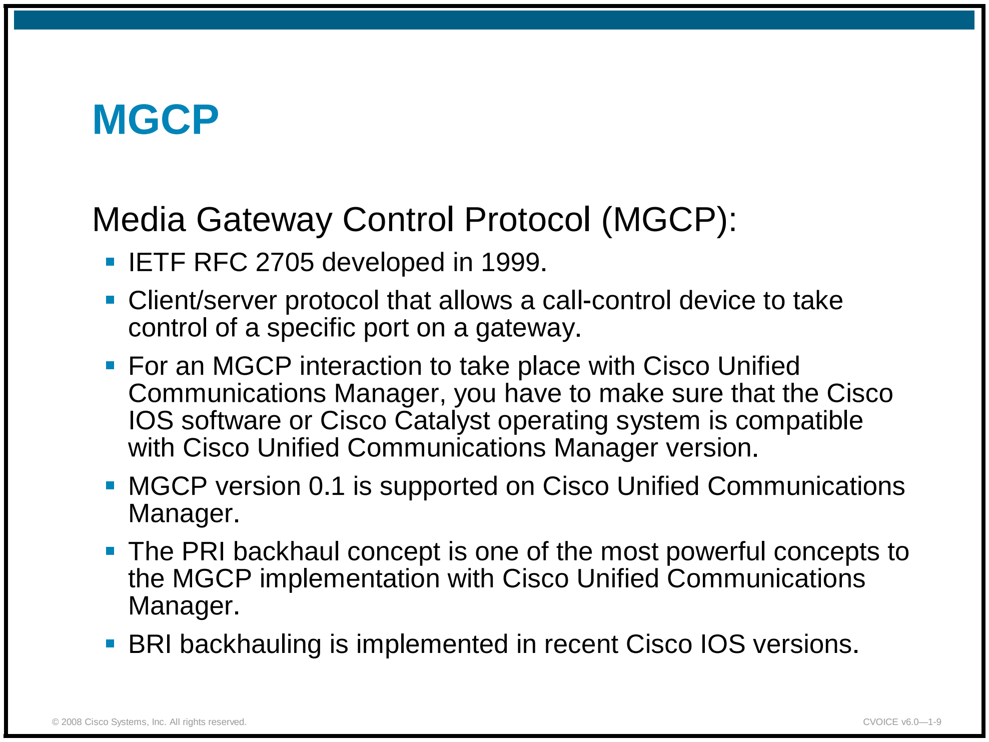
- **Audio codecs:** An audio codec encodes the audio signal from the microphone for transmission on the transmitting H.323 terminal and decodes the received audio code that is sent to the speaker on the receiving H.323 terminal. Because audio is the minimum service provided by the H.323 standard, all H.323 terminals must have at least one audio codec support, as specified in the ITU-T G.711 recommendation (audio coding at 64 kb/s). Additional audio codec recommendations such as G.722 (64, 56, and 48 kb/s), G.723.1 (5.3 and 6.3 kb/s), G.728 (16 kb/s), and G.729 (8 kb/s) may also be supported.
- **Video codecs:** A video codec encodes video from the camera for transmission on the transmitting H.323 terminal and decodes the received video code that is sent to the video display on the receiving H.323 terminal. Because H.323 specifies support of video as optional, the support of video codecs is optional as well. However, any H.323 terminal providing video communications must support video encoding and decoding as specified in the ITU-T H.261 recommendation.

In IP communications environments, H.323 is widely used with gateways, gatekeepers, and third-party H.323 clients, especially video terminals. Connections are configured between devices using static destination IP addresses.

Note Because H.323 is a peer-to-peer protocol, H.323 gateways are not registered with Cisco Unified Communications Manager as an endpoint. An IP address is configured in the Cisco Unified Communications Manager to confirm that communication is possible.

Media Gateway Control Protocol

This subtopic covers MGCP.



MGCP

Media Gateway Control Protocol (MGCP):

- IETF RFC 2705 developed in 1999.
- Client/server protocol that allows a call-control device to take control of a specific port on a gateway.
- For an MGCP interaction to take place with Cisco Unified Communications Manager, you have to make sure that the Cisco IOS software or Cisco Catalyst operating system is compatible with Cisco Unified Communications Manager version.
- MGCP version 0.1 is supported on Cisco Unified Communications Manager.
- The PRI backhaul concept is one of the most powerful concepts to the MGCP implementation with Cisco Unified Communications Manager.
- BRI backhauling is implemented in recent Cisco IOS versions.

MGCP is a client-server call control protocol built on centralized control architecture. This centralized control architecture has the advantage of centralized gateway administration and provides for largely scalable IP telephony solutions. All the dial plan information resides on a separate call agent. The call agent, which controls the ports on the gateway, performs call control. The gateway does media translation between the PSTN and the VoIP networks for external calls. In a Cisco network, Cisco Unified Communications Manager systems function as the call agents.

MGCP is a plain-text protocol used by call control devices to manage IP telephony gateways. MGCP was defined under RFC 2705 (Media Gateway Control Protocol [MGCP] Version 1.0.), which was updated by RFC 3660 (Basic Media Gateway Control Protocol [MGCP] Packages), and superseded by RFC 3435 (Media Gateway Control Protocol [MGCP] Version 1.0), which was updated by RFC 3661 (Media Gateway Control Protocol [MGCP] Return Code Usage).

With this protocol, the Cisco Unified Communications Manager knows of and controls individual voice ports on the gateway. MGCP allows complete control of the dial plan from Cisco Unified Communications Manager, and gives Cisco Unified Communications Manager per-port control of connections to the PSTN, legacy PBX, voice-mail systems, plain old telephone service (POTS) phones, and so forth. This control is implemented by a series of plain-text commands sent over UDP port 2427 between the Cisco Unified Communications Manager and the gateway. A list of the possible commands and their functions is provided later in this lesson.

It is important to note that for an MGCP interaction to take place with Cisco Unified Communications Manager, the gateway must have Cisco Unified Communications Manager support. If you are a registered customer of the Software Advisor, you can use this tool to make sure that your platform and your Cisco IOS software or Cisco Catalyst operating system version are compatible with Cisco Unified Communications Manager for MGCP. Also, make sure that your version of Cisco Unified Communications Manager supports the gateway.

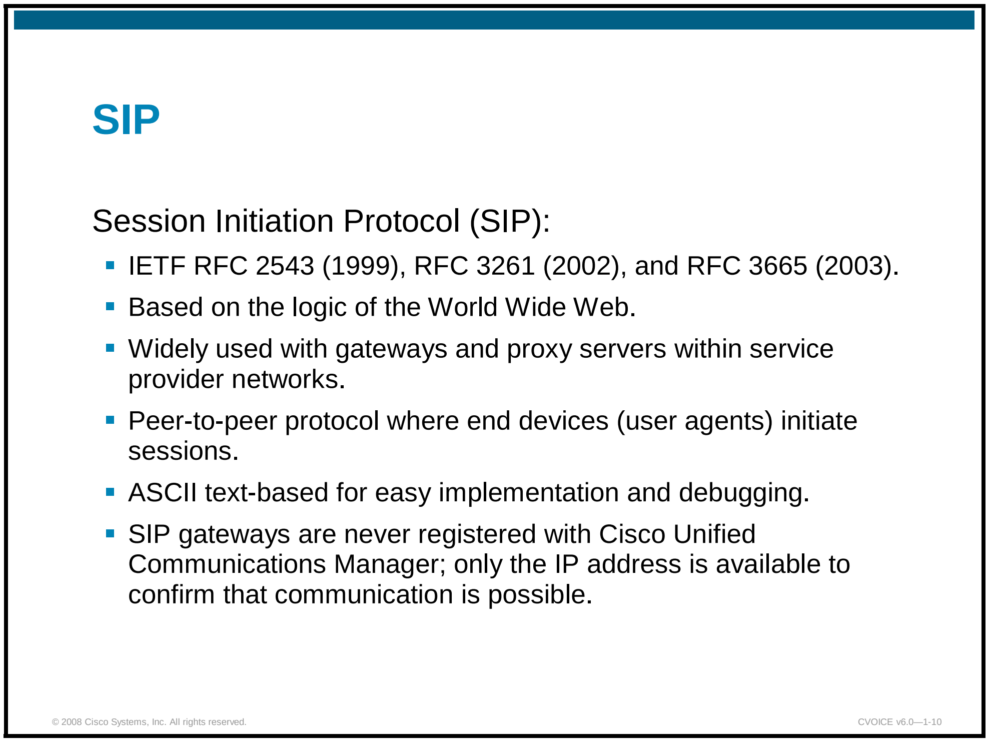
PRI and BRI Backhaul

A PRI and BRI backhaul is an internal interface between the call agent (such as Cisco Unified Communications Manager) and Cisco gateways. It is a separate channel for backhauling signaling information. A PRI backhaul forwards PRI Layer 3 (Q.931) signaling information via a TCP connection.

An MGCP gateway is relatively easy to configure. Because the call agent has all the call-routing intelligence, you do not need to configure the gateway with all the dial peers it would otherwise need. A downside is that a call agent must always be available. Cisco MGCP gateways can use Survivable Remote Site Telephony (SRST) and MGCP fallback to allow the H.323 protocol to take over and provide local call routing in the absence of a Cisco Unified Communications Manager. In that case, you must configure dial peers on the gateway for use by H.323.

Session Initiation Protocol

This subtopic covers SIP.



SIP

Session Initiation Protocol (SIP):

- IETF RFC 2543 (1999), RFC 3261 (2002), and RFC 3665 (2003).
- Based on the logic of the World Wide Web.
- Widely used with gateways and proxy servers within service provider networks.
- Peer-to-peer protocol where end devices (user agents) initiate sessions.
- ASCII text-based for easy implementation and debugging.
- SIP gateways are never registered with Cisco Unified Communications Manager; only the IP address is available to confirm that communication is possible.

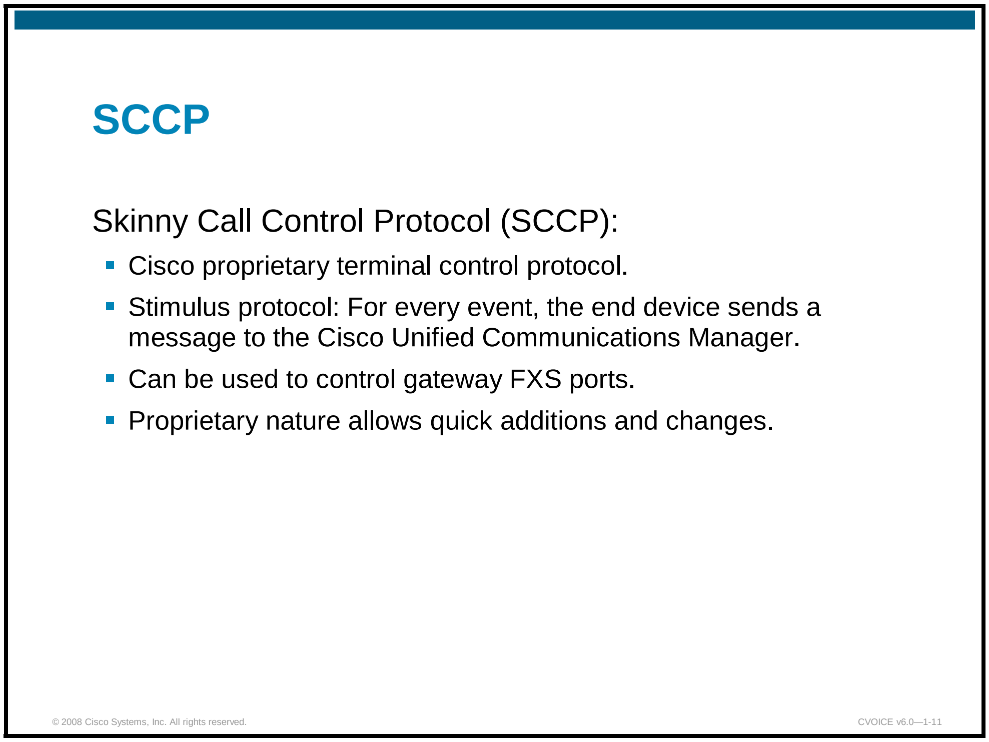
SIP is a protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) working group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999; RFC 3261, published in June 2002; and RFC 3665, published in December 2003. Because it is a common standard based on the logic of the World Wide Web and very simple to implement, SIP is widely used with gateways and proxy servers within service provider networks for internal and end-customer signaling.

SIP is a peer-to-peer protocol where user agents (UAs) initiate sessions, like H.323. But unlike H.323, SIP uses ASCII text-based messages to communicate. Therefore, you can implement and troubleshoot it very easily, and analyze the incoming signaling traffic content very simply.

Because SIP is a peer-to-peer protocol, the Cisco Unified Communications Manager does not control SIP devices, and SIP devices do not register with Cisco Unified Communications Manager. As with H.323 gateways, only the IP address is available on Cisco Unified Communications Manager to confirm that communication between the Cisco Unified Communications Manager and the SIP voice gateway is possible.

Skinny Call Control Protocol

This subtopic covers SCCP.



SCCP

Skinny Call Control Protocol (SCCP):

- Cisco proprietary terminal control protocol.
- Stimulus protocol: For every event, the end device sends a message to the Cisco Unified Communications Manager.
- Can be used to control gateway FXS ports.
- Proprietary nature allows quick additions and changes.

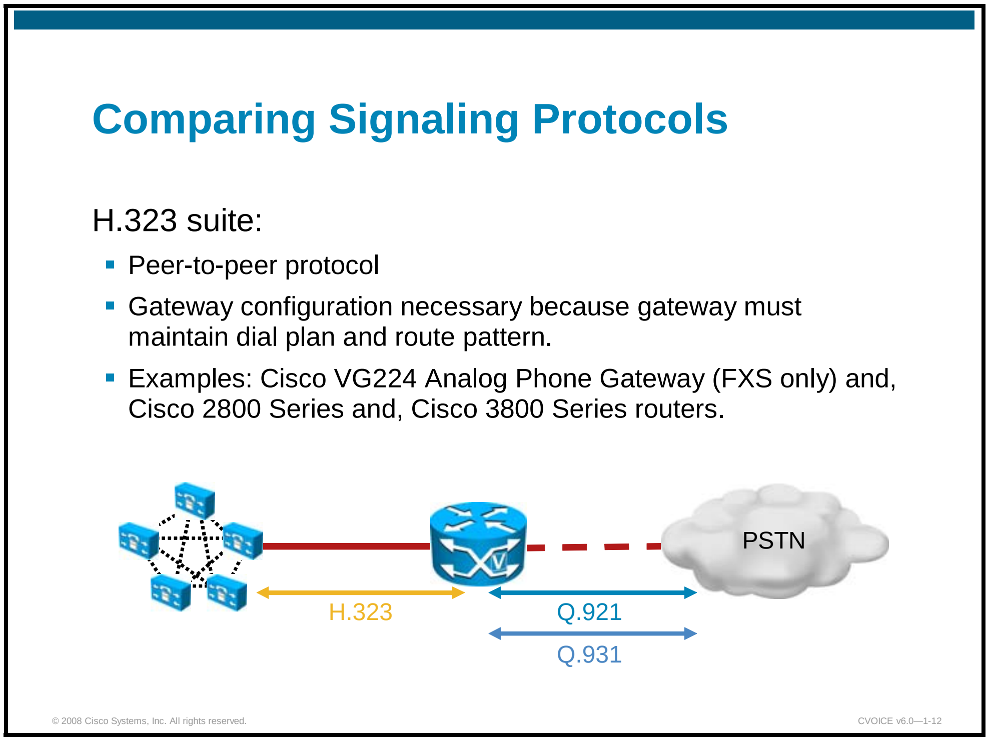
CVOICE v6.0—1-11

SCCP is a Cisco proprietary protocol that is used for the communications between Cisco Unified Communications Manager and terminal endpoints. SCCP is a stimulus protocol, meaning any event (such as the phone is on hook or off hook, buttons have been pressed, and so on) causes a message to be sent to the Cisco Unified Communications Manager. The Cisco Unified Communications Manager then sends specific instructions back to the device to tell it what to do about the event. Therefore, each press on a phone button causes data traffic between the Cisco Unified Communications Manager and the terminal endpoint. SCCP is widely used with Cisco IP phones. The major advantage of SCCP within Cisco Unified Communications Manager networks is its proprietary nature, which allows you to make quick changes to the protocol and add features and functionality.

SCCP is a simplified protocol used in VoIP networks. Cisco IP phones that use SCCP can coexist in an H.323 environment. When used with Cisco Communications Manager, the SCCP client can interoperate with H.323-compliant terminals.

Comparing VoIP Signaling Protocols

This topic describes the differences between the gateway signaling protocols that are commonly used within VoIP environments.



Comparing Signaling Protocols

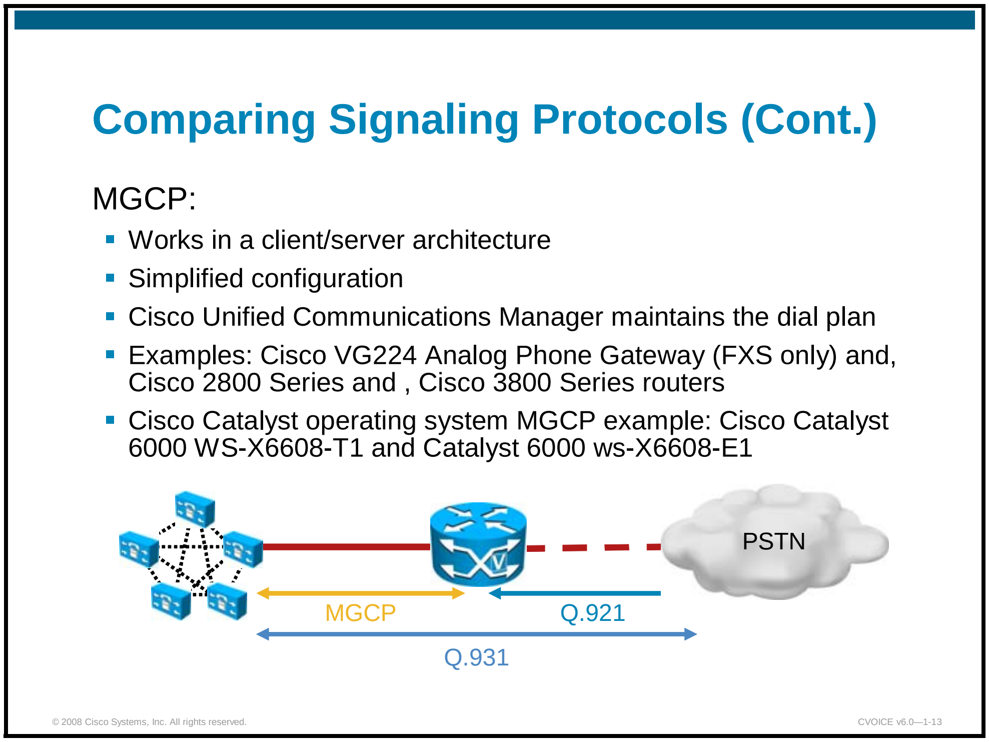
H.323 suite:

- Peer-to-peer protocol
- Gateway configuration necessary because gateway must maintain dial plan and route pattern.
- Examples: Cisco VG224 Analog Phone Gateway (FXS only) and, Cisco 2800 Series and, Cisco 3800 Series routers.

CVOICE v6.0—1-12

The H.323 protocol suite is a peer-to-peer protocol. The necessary gateway configuration is relatively complex because you need to define the dial plan and route patterns directly on the gateway. Examples of H.323-capable devices are the Cisco VG224 Analog Phone Gateway and the Cisco 2600XM Series Multiservice Routers, 2800 Series Integrated Services Routers, 3700 Series Multiservice Access Routers, and 3800 Series Integrated Services Routers.

The H.323 protocol is responsible for the entire signaling between the Cisco Unified Communications Manager cluster and the gateway. The ISDN protocols, Q.921 and Q.931, are used only on the ISDN link to the PSTN.



Comparing Signaling Protocols (Cont.)

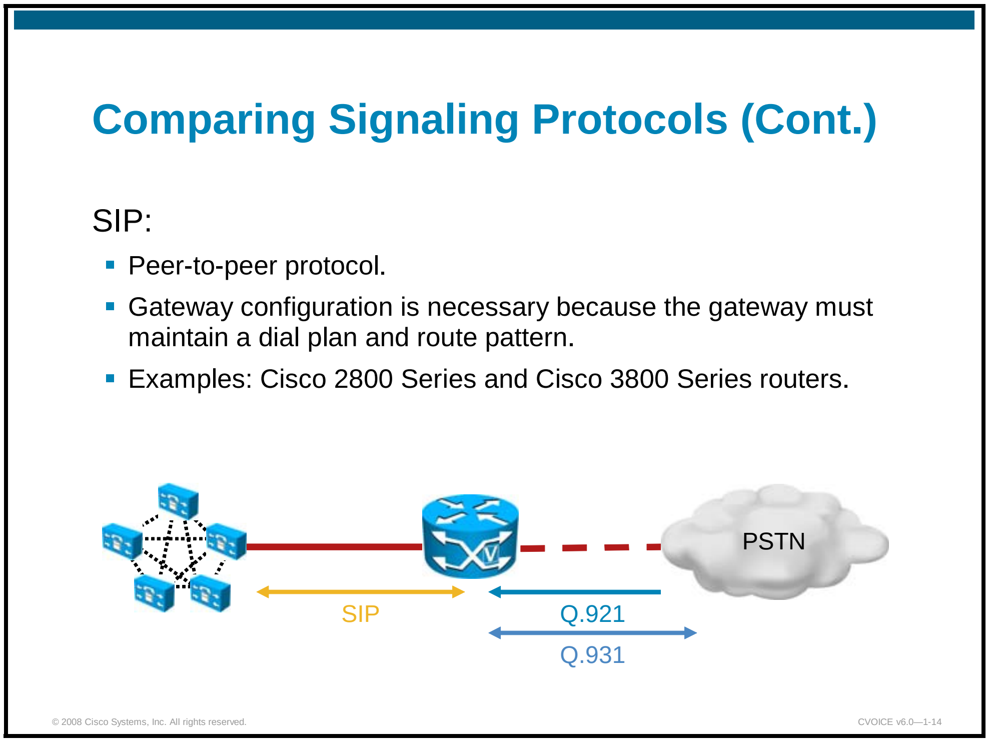
MGCP:

- Works in a client/server architecture
- Simplified configuration
- Cisco Unified Communications Manager maintains the dial plan
- Examples: Cisco VG224 Analog Phone Gateway (FXS only) and, Cisco 2800 Series and , Cisco 3800 Series routers
- Cisco Catalyst operating system MGCP example: Cisco Catalyst 6000 WS-X6608-T1 and Catalyst 6000 ws-X6608-E1

CVOICE v6.0—1-13

The MGCP protocol is based on a client/server architecture. That simplifies the configuration because the dial plan and route patterns are defined directly on the Cisco Unified Communications Manager within the cluster. Examples of MGCP-capable devices are the VG224 Analog Phone Gateway and the Cisco 2600XM Series, 2800 Series, 3700 Series, and 3800 Series routers. Cisco Catalyst operating system MGCP gateways include the Cisco Catalyst 6000 WS-6608-E1 and Catalyst 6000 WS-6608-T1.

MGCP is used to manage the gateway. All ISDN Layer 3 information is backhauled to the Cisco Unified Communications Manager. Only the ISDN Layer 2 information (Q.921) is terminated on the gateway.



Comparing Signaling Protocols (Cont.)

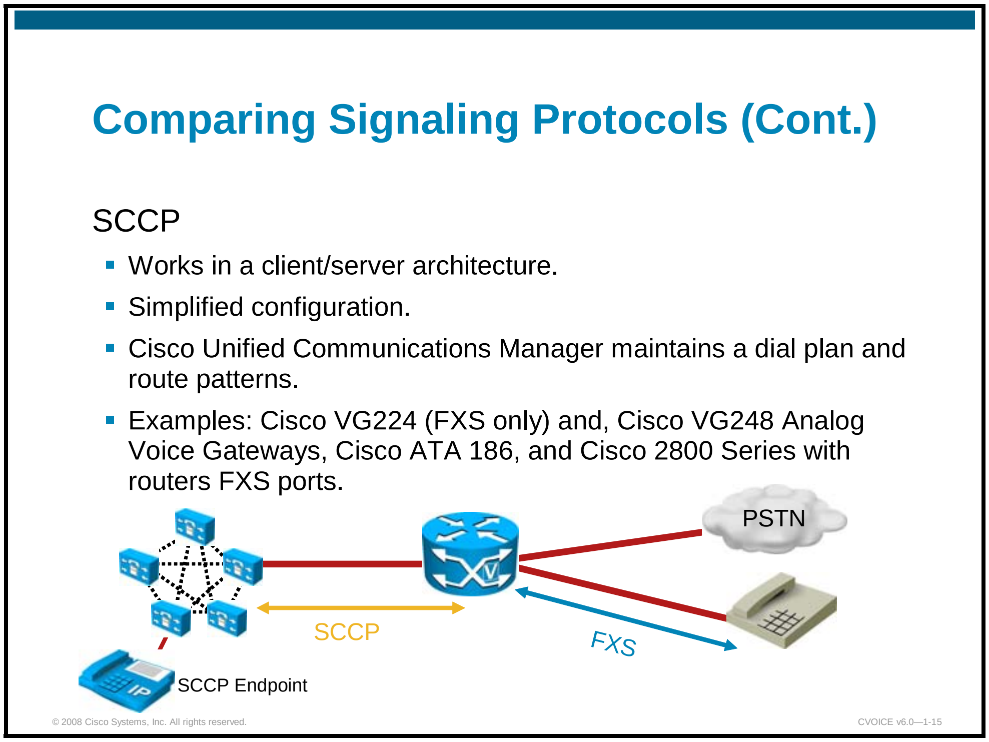
SIP:

- Peer-to-peer protocol.
- Gateway configuration is necessary because the gateway must maintain a dial plan and route pattern.
- Examples: Cisco 2800 Series and Cisco 3800 Series routers.

CVOICE v6.0—1-14

Like the H.323 protocol, SIP is a peer-to-peer protocol. The necessary gateway configuration is relatively complex because the dial plan and route patterns need to be defined directly on the gateway. Examples of SIP-capable devices are the Cisco 2800 Series and 3800 Series routers.

The SIP protocol is responsible for the entire signaling between the Cisco Unified Communications Manager cluster and the gateway. The ISDN protocols, Q.921 and Q.931, are used only on the ISDN link to the PSTN.



Comparing Signaling Protocols (Cont.)

SCCP

- Works in a client/server architecture.
- Simplified configuration.
- Cisco Unified Communications Manager maintains a dial plan and route patterns.
- Examples: Cisco VG224 (FXS only) and, Cisco VG248 Analog Voice Gateways, Cisco ATA 186, and Cisco 2800 Series with routers FXS ports.

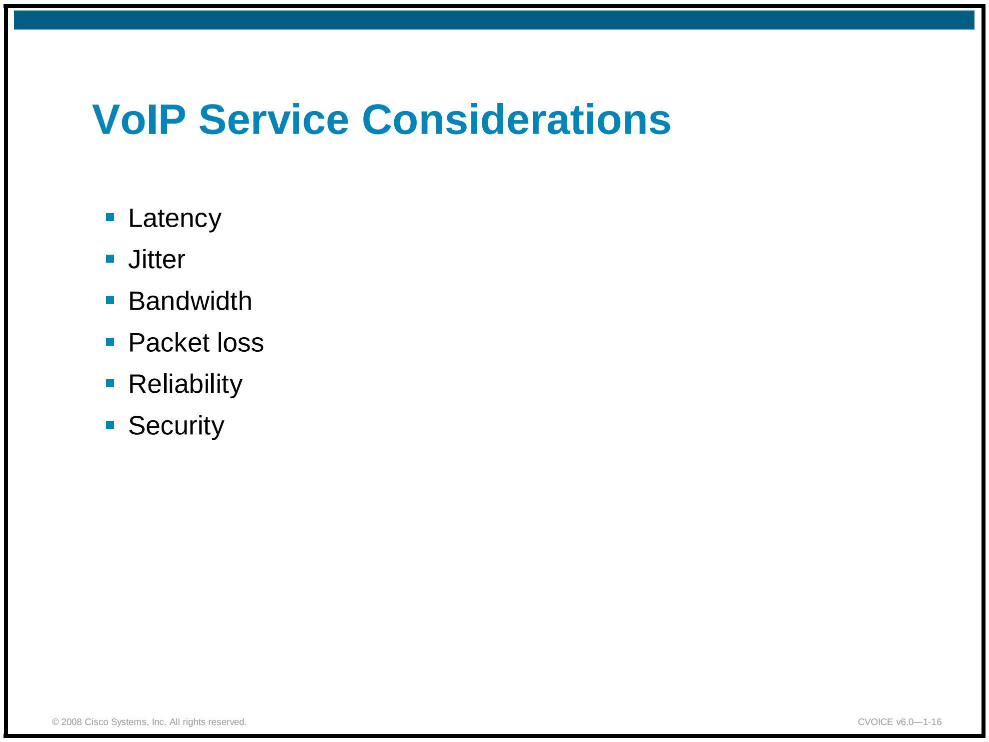
CVOICE v6.0—1-15

SCCP works in a client/server architecture. Therefore, it simplifies the configuration of SCCP devices such as Cisco IP phones and Cisco Analog Telephone Adaptor (ATA) 180 Series and Cisco Voice Gateway 200 (VG200) Series Gateways with a Foreign Exchange Station (FXS).

SCCP is used on Cisco VG224 and VG248 Analog Phone Gateways. Analog telephone adaptors (ATAs) enable communications between Cisco Unified Communications Manager and the gateway. The gateway then uses standard analog signaling to the analog device connected to the FXS port. Recent versions of Cisco IOS voice gateways, for example, the 2800 Series, also support SCCP-controlled FXS ports.

VoIP Service Considerations

This topic describes issues that can affect voice delivery in an IP network.



VoIP Service Considerations

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

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—1-16

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

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

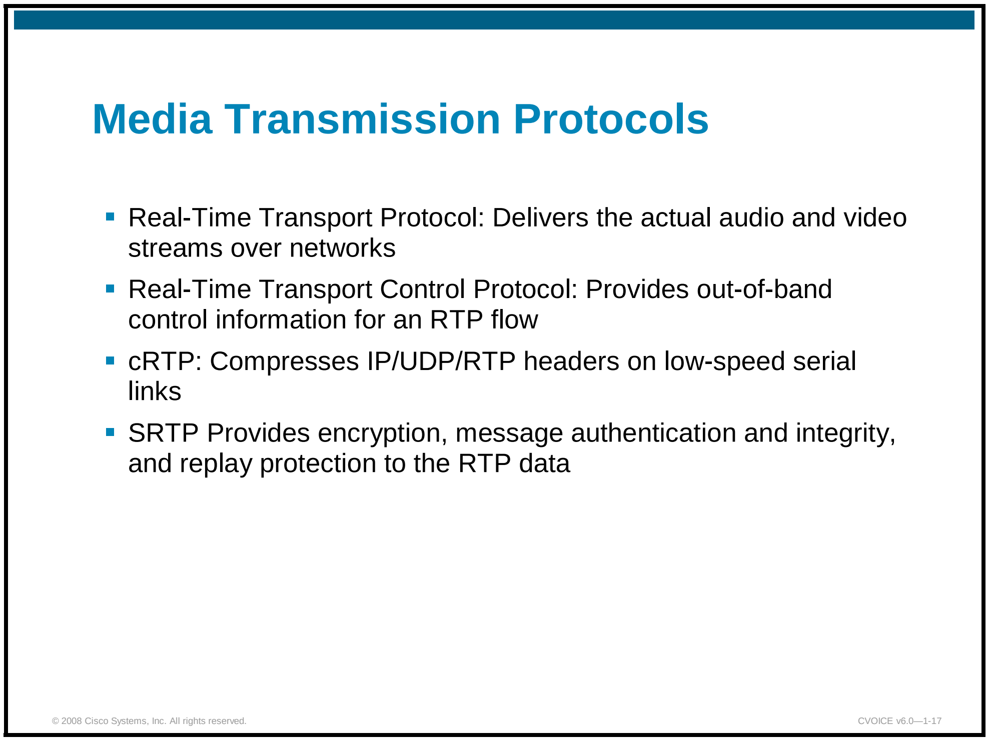
Issues and Solutions for VoIP in a Converged Network

Issue	Solution
Latency	■ Increase bandwidth ■ Choose a different codec type ■ Fragment data packets ■ Prioritize voice packets
Jitter	■ Use dejitter buffers
Bandwidth	■ Calculate bandwidth requirements, including voice payload, overhead, and data

Issue	Solution
Packet loss	■ Design the network to minimize congestion ■ Prioritize voice packets ■ Use codecs to minimize small amounts of packet loss
Reliability	■ Provide redundancy for these components: — Hardware — Links — Power (uninterruptible power supply [UPS]) ■ Perform proactive network management
Security	■ Secure these components: — Network infrastructure — Call-processing systems — Endpoints — Applications

Media Transmission Protocols

This topic describes the characteristics of the protocols that are used for media transmission in a VoIP network.



Media Transmission Protocols

- Real-Time Transport Protocol: Delivers the actual audio and video streams over networks
- Real-Time Transport Control Protocol: Provides out-of-band control information for an RTP flow
- cRTP: Compresses IP/UDP/RTP headers on low-speed serial links
- SRTP Provides encryption, message authentication and integrity, and replay protection to the RTP data

CVOICE v6.0—1-17

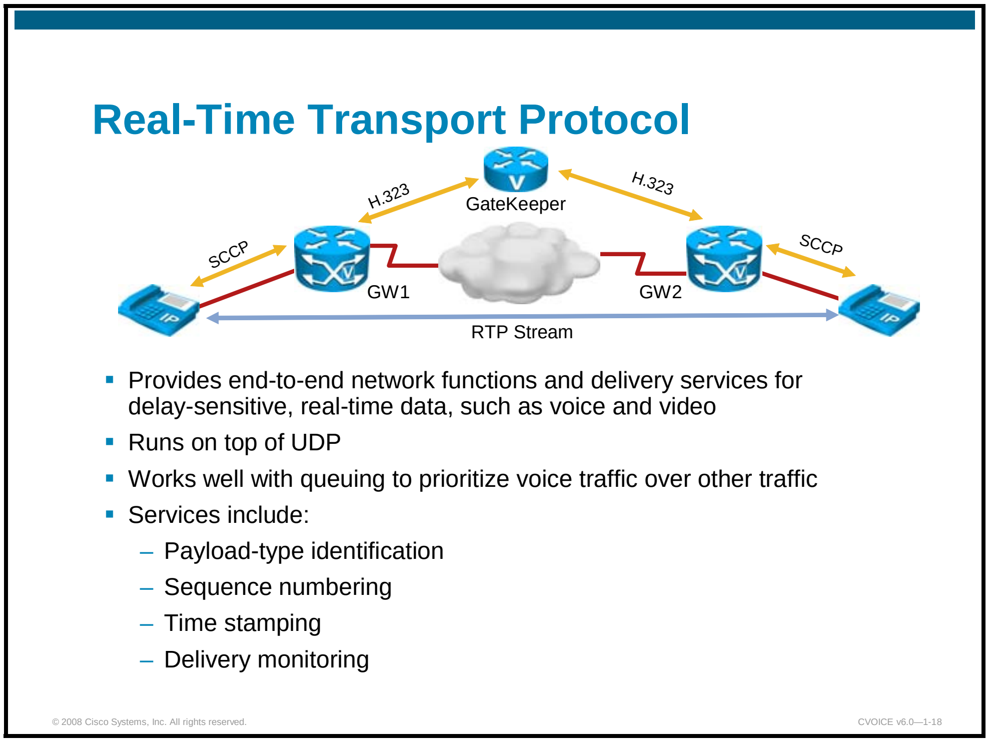
In a VoIP network, the actual voice data (conversations) are transported across the transmission media using Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP). RTP defines a standardized packet format for delivering audio and video over the Internet. RTCP is a companion protocol to RTP as it provides for the delivery of control information for individual RTP streams. Compressed Real-Time Transport Protocol (cRTP) and Secure Real-Time Transport Protocol (SRTP) were developed to enhance the use of RTP.

Datagram protocols, such as UDP, send the media stream as a series of small packets. This is simple and efficient; however, packets can be lost or corrupted in transit. Depending on the protocol and the extent of the loss, the client may be able to recover the data with error correction techniques, may interpolate over the missing data, or may suffer a data dropout. RTP and the RTCP were specifically designed to stream media over networks. They are both built on top of UDP.

The following subtopics cover RTP and its related protocols RTCP, cRTP, and SRTP.

Real-Time Transport Protocol

This subtopic covers RTP.



Real-Time Transport Protocol

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

RTP defines a standardized packet format for delivering audio and video over the Internet. It was developed by the Audio/Video Transport Working Group of the IETF and first published in 1996 as RFC 1889, which was made obsolete in 2003 by RFC 3550.

RTP provides end-to-end network transport functions that are 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 so that it can use the multiplexing and checksum services of that protocol. RTP does not have a standard TCP or UDP port on which it communicates. The only standard that it obeys is that UDP communications are done via an even port, and the next higher odd port is used for RTCP communications. Although there are no standards assigned, RTP is generally configured to use ports 16384 to 32767.

RTP can carry any data with real-time characteristics, such as interactive audio and video. Call setup and teardown is usually performed by SIP. The fact that RTP uses a dynamic port range makes it difficult for it to traverse firewalls.

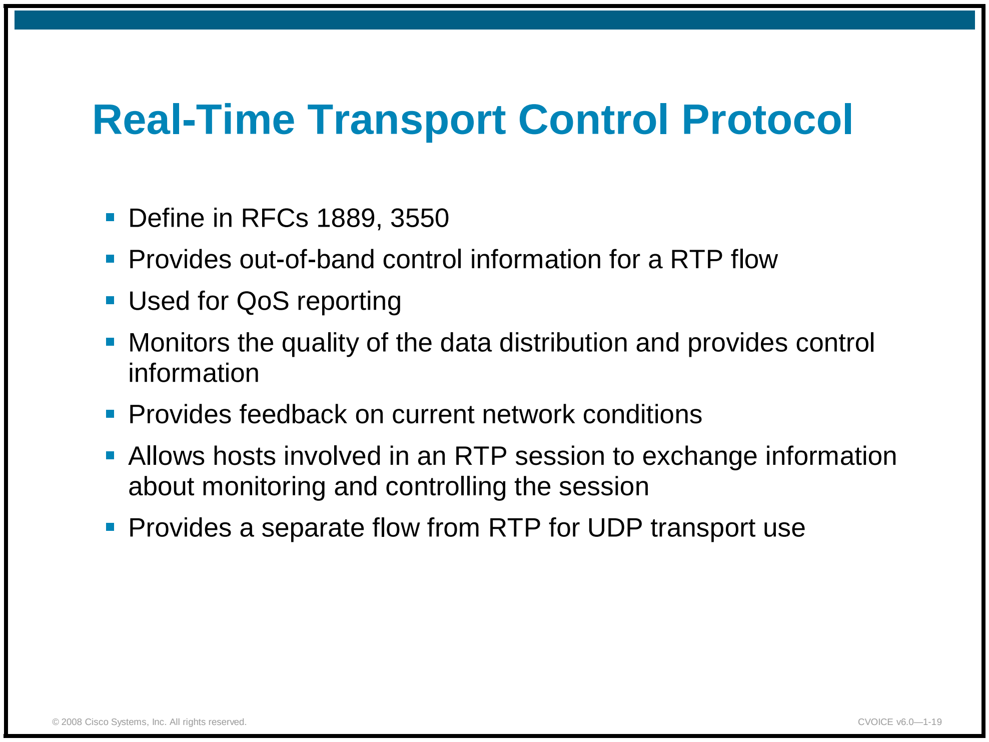
Although RTP is often used for unicast sessions, it is primarily designed for multicast sessions. In addition to the roles of sender and receiver, RTP also defines the roles of translator and mixer to support the multicast requirements.

RTP is frequently used in conjunction with Real Time Streaming Protocol (RTSP) in streaming media systems. RTP is also used in conjunction with H.323 or SIP in videoconferencing and push-to-talk systems. These two characteristics make RTP the technical foundation of the VoIP industry. RTP goes along with RTCP, and it is built on top of UDP. Applications that use RTP are less sensitive to packet loss but are typically very sensitive to delays, so UDP is a better choice than TCP for such applications.

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

Real-Time Transport Control Protocol

This subtopic covers RTCP.



Real-Time Transport Control Protocol

- Define in RFCs 1889, 3550
- Provides out-of-band control information for a RTP flow
- Used for QoS reporting
- Monitors the quality of the data distribution and provides control information
- Provides feedback on current network conditions
- Allows hosts involved in an RTP session to exchange information about monitoring and controlling the session
- Provides a separate flow from RTP for UDP transport use

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-19

RTCP is a sister protocol of the RTP. It was first defined in RFC 1889, which was replaced by RFC 3550. RTP provides out-of-band control information for an RTP flow. It works along side RTP in the delivery and packaging of multimedia data, but it does not transport any data itself. Although it is used periodically to transmit control packets to participants in a streaming multimedia session, the primary function of RTCP is to provide feedback on the quality of service being provided by RTP.

RTCP is used for QoS reporting. It gathers statistics on a media connection and information such as bytes sent, packets sent, lost packets, jitter, feedback, and round-trip delay. Applications use this information to increase the quality of service by perhaps limiting flow or using a low-compression codec instead of a high-compression codec.

There are several types of RTCP packets: sender report packet, receiver report packet, source description RTCP packet, goodbye RTCP packet, and application-specific RTCP packet.

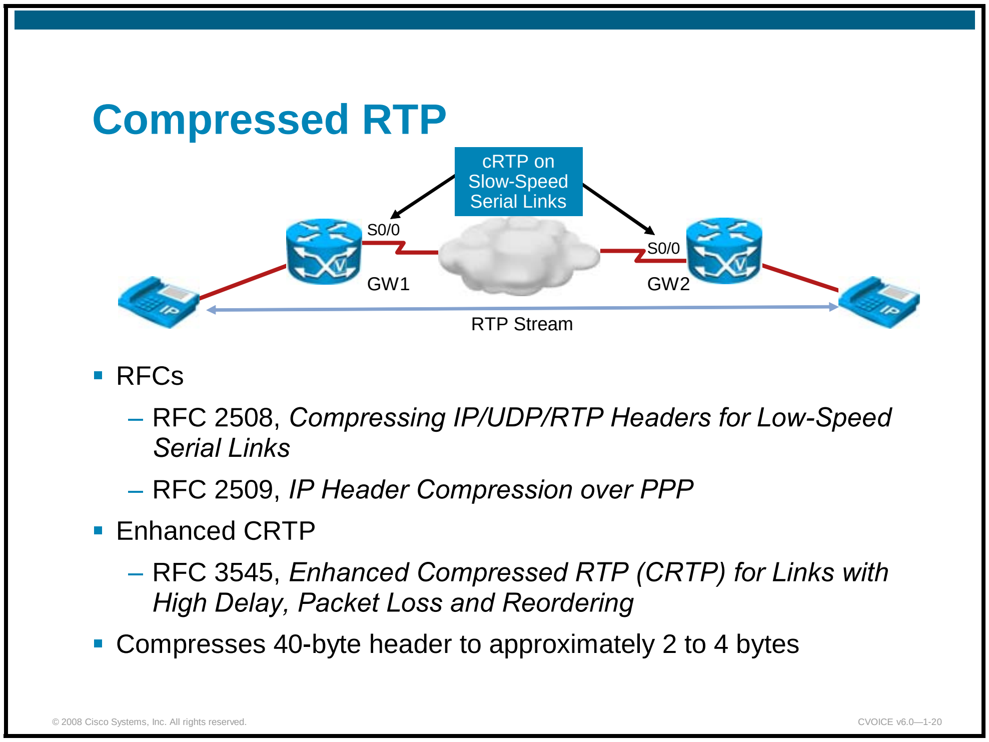
RTCP provides the following feedback on current network conditions:

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

RTCP is assigned the next odd-numbered port. Each voice call has four ports assigned: RTP plus RTCP in the transmit direction and RTP plus RTCP in the receive direction.

Compressed RTP

This subtopic covers cRTP.



Compressed RTP

- RFCs
  - RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*
  - RFC 2509, *IP Header Compression over PPP*
- Enhanced CRTP
  - RFC 3545, *Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering*
- Compresses 40-byte header to approximately 2 to 4 bytes

CVOICE v6.0—1-20

RTP includes a data portion and a header portion. The data portion of RTP is a thin protocol that provides support for the real-time properties of applications, such as continuous media, including timing reconstruction, loss detection, and content identification. The header portion of RTP is considerably larger than the data portion. The header portion consists of an IP segment, a UDP segment, and an RTP segment. Given the size of the IP/UDP/RTP segment combinations, it is inefficient to send the IP/UDP/RTP header without compressing it.

The minimum 20 bytes of the IP segment, combined with the 8 bytes of the UDP segment and the 12 bytes of the RTP segment, create a 40-byte IP/UDP/RTP header. The RTP packet has a payload of approximately 20 to 150 bytes for audio applications that use compressed payloads.

The RTP header compression feature compresses the IP/UDP/RTP header in an RTP data packet from 40 bytes to approximately 2 to 4 bytes.

Compressed RTP, specified in RFCs 2508, 2509, and 3545, was developed to decrease the size of the IP, UDP, and RTP headers.

The RFCs are detailed here:

- RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*
- RFC 2509, *IP Header Compression over PPP*
- RFC 3545, *Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering*

RFC 2509 was designed to work with reliable and fast point-to-point links. In less than optimal circumstances, where there may be long delays, packet loss, and out-of-sequence packets, cRTP does not function well for VoIP applications. Another adaptation, Enhanced CRPT (ECRPT), was defined in a subsequent Internet Draft document to overcome that problem.

RTP header compression is supported on serial lines using Frame Relay, High-Level Data Link Control (HDLC), or PPP encapsulation. It is also supported over ISDN interfaces.

Why and When to Use cRTP

RTP header compression accomplishes major gains in terms of packet compression because although several fields in the header change in every packet, the difference from packet to packet is often constant. Therefore, the second-order difference is zero. The decompressor can reconstruct the original header without any loss of information.

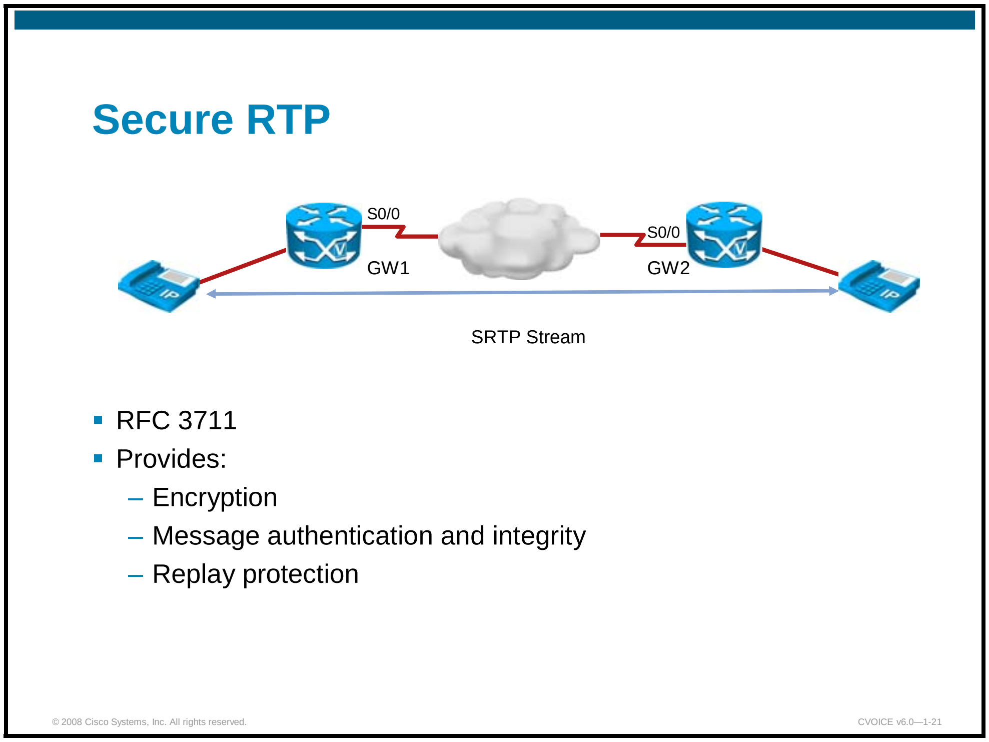
RTP header compression also reduces overhead for multimedia RTP traffic. The reduction in overhead results in a corresponding reduction in delay. RTP header compression is especially beneficial when the RTP payload size is small, for example, for compressed audio payloads of 20 to 50 bytes.

Use RTP header compression on any WAN interface where you are concerned about bandwidth and where there is a high volume of RTP traffic. RTP header compression can be used for media-on-demand and interactive services such as Internet telephony. RTP header compression provides support for real-time conferencing of groups of any size within the Internet. This support includes source identification support for gateways such as audio and video bridges, and support for multicast-to-unicast translators. RTP header compression can benefit both telephony voice and multicast backbone applications running over slow links.

Note Using RTP header compression on any high-speed interfaces—that is, anything over T1 speed—is not recommended. Any bandwidth savings achieved with RTP header compression may be offset by an increase in CPU utilization on the router.

Secure RTP

This subtopic covers SRTP.



Secure RTP

- RFC 3711
- Provides:
  - Encryption
  - Message authentication and integrity
  - Replay protection

CVOICE v6.0—1-21

SRTP was first published by the IETF in March 2004 as RFC 3711, and it was designed to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications.

SRTP also has a sister protocol, called Secure RTCP (SRTCP). SRTCP provides the same security-related features to RTCP as the ones provided by SRTP to RTP. SRTP can be used in conjunction with compressed RTP.

Flow Encryption

SRTP standardizes the utilization of only a single cipher, Advanced Encryption Standard (AES), which can be used in two cipher modes and turns the original AES cipher block into a stream cipher.

- **Segmented integer counter (SIC) mode:** A counter mode that allows random access to any block and is essential for RTP traffic running over an unreliable network with possible loss of packets. AES running in this mode is the default encryption algorithm, with a default encryption key length of 128 bits and a default session salt key length of 112 bits.
- **f8-mode:** A variation of output feedback mode. The default values of the encryption key and salt key are the same as for AES in Counter Mode.

In addition to the AES cipher, SRTP gives the user the ability to disable encryption outright, using the "NULL cipher." Actually, the NULL cipher does not perform any encryption—the encryption algorithm functions as though the key stream contains only zeroes and copies the input stream to the output stream without any changes.

Note It is mandatory for this cipher mode to be implemented in any SRTP-compatible system. As such, it can be used when the confidentiality guarantees ensured by SRTP are not required, while other SRTP features (such authentication and message integrity) may be used.

Because encryption algorithms do not secure message integrity themselves, allowing the attacker to either forge the data or at least to replay previously transmitted data, SRTP also provides the means to secure the integrity of data and safety from replay.

Authentication and Integrity

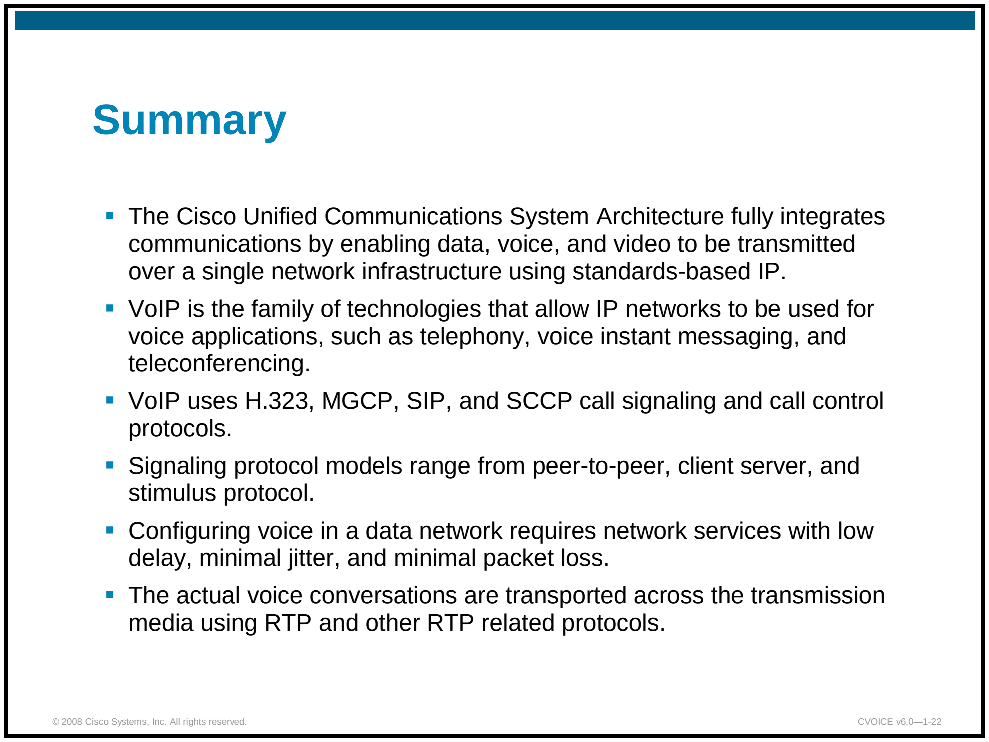
Hashed Message Authentication Code-Secure Hash Algorithm 1 (HMAC-SHA-1) (defined in RFC 2104) is used to authenticate the message and protect its integrity. This method produces a 160-bit result, which is then truncated to 80 bits to become the authentication tag that is then appended to the packet. The HMAC is calculated over the packet payload and material from the packet header, including the packet sequence number.

Replay Protection

To protect against replay attacks, the receiver must maintain the indices of previously received messages, comparing them with the index of each newly received message and admitting the new message only if it has not been played before. Such an approach heavily relies on the integrity protection being enabled (to make it impossible to spoof message indices).

Summary

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



Summary

- The Cisco Unified Communications System Architecture fully integrates communications by enabling data, voice, and video to be transmitted over a single network infrastructure using standards-based IP.
- VoIP is the family of technologies that allow IP networks to be used for voice applications, such as telephony, voice instant messaging, and teleconferencing.
- VoIP uses H.323, MGCP, SIP, and SCCP call signaling and call control protocols.
- Signaling protocol models range from peer-to-peer, client server, and stimulus protocol.
- Configuring voice in a data network requires network services with low delay, minimal jitter, and minimal packet loss.
- The actual voice conversations are transported across the transmission media using RTP and other RTP related protocols.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-22

Lesson Self-Check

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

Q1) The Cisco Unified Communications system fully integrates communications by enabling ________, _________, and ________ to be transmitted over a single network infrastructure using standards-based IP.

Relates to: Cisco Unified Communications Architecture

Q2) VoIP is a ___________ of technologies.

Relates to: VoIP Overview

Q3) VoIP uses _______, _______, ________, and _______ call signaling and call control protocols.

Relates to: VoIP Signaling Protocols

Q4) Signaling protocol models range from __________, __________, and __________ protocols.

Relates to: Comparing VoIP Signaling Protocols

Q5) Factors to consider when configuring voice in a data network include________, ________, and ________ loss.

Relates to: VoIP Service Considerations

Q6) Protocols used for the actual voice conversations include ______, ______, ______, and ______.

Relates to: Media Transmission Protocols

Lesson Self-Check Answer Key

Q1) data, voice, video

Q2) family

Q3) H.323, SIP, MGCP, SCCP

Q4) peer-to-peer, client/server, stimulus

Q5) delay, jitter, packet

Q6) RTP, RTCP, cRTP, SRTP

Lesson 2

Introducing Voice Gateways

Overview

Gateways provide a number of ways to connect an IP telephony network to the public switched telephone network (PSTN), a legacy PBX, key systems, or other time-division multiplexing (TDM) systems. Gateways range from specialized, entry-level, and standalone voice gateways, to high-end, integrated routers and Cisco IOS gateways. This lesson introduces voice gateways and deployment models in an IP telephony network.

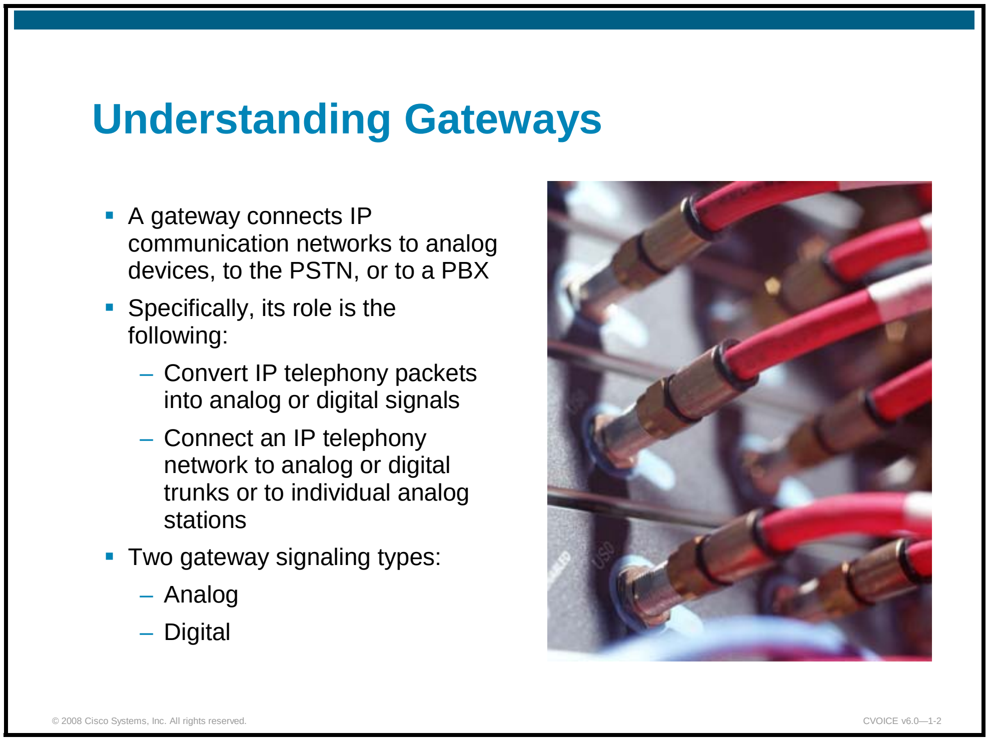
Objectives

Upon completing this lesson, you will be able to describe the different types of voice gateways and when to use each type. This ability includes being able to meet these objectives:

- Describe the functionality of gateways and their role of connecting VoIP to traditional PSTN and telephony equipment
- Describe the different Cisco gateway platforms
- Identify supported IP telephony deployment models
- Identify the major characteristics and design guidelines of a single-site IP telephony deployment model
- Identify the major characteristics and design guidelines of a multisite centralized IP telephony deployment model
- Identify the major characteristics and design guidelines of a multisite distributed IP telephony deployment model
- Identify the characteristics, limitations, and advantages of clustering over the IP WAN

Understanding Gateways

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



Understanding Gateways

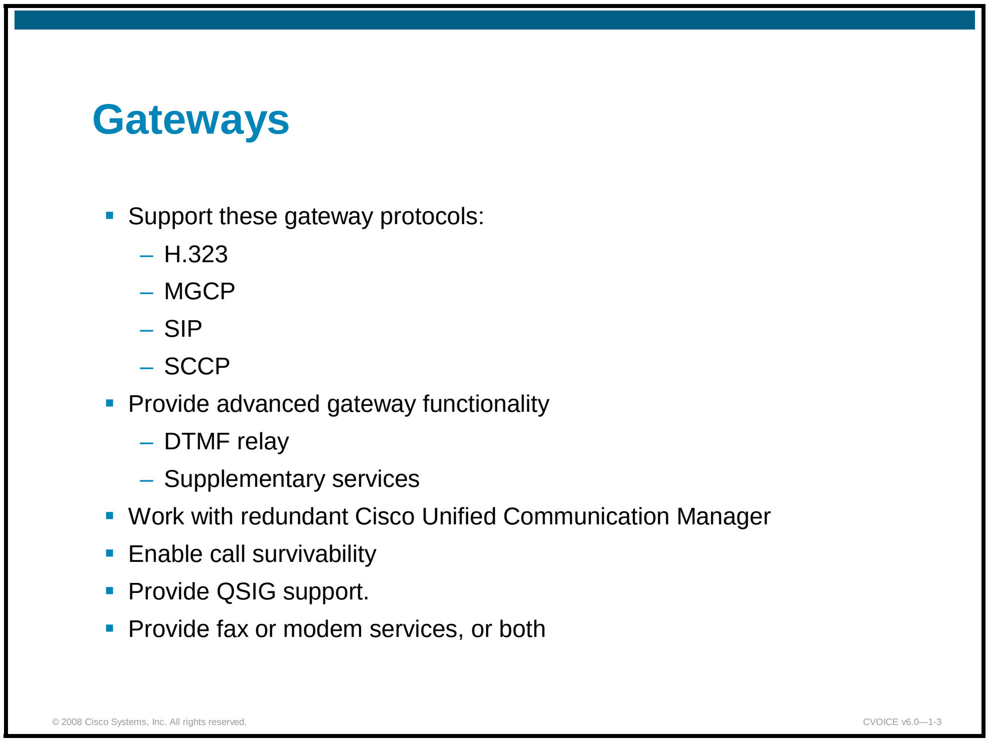
- A gateway connects IP communication networks to analog devices, to the PSTN, or to a PBX
- Specifically, its role is the following:
  - Convert IP telephony packets into analog or digital signals
  - Connect an IP telephony network to analog or digital trunks or to individual analog stations
- Two gateway signaling types:
  - Analog
  - Digital

CVOICE v6.0—1-2

A voice gateway functions as a translator between different types of networks. Gateways allow terminals of one type, such as H.323, to communicate with terminals of another type, such as a PBX, by converting protocols. Gateways connect a company network to the PSTN, a PBX, or individual analog devices such as a phone or fax.

These are the two types of Cisco access gateways:

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



Gateways

- Support these gateway protocols:
  - H.323
  - MGCP
  - SIP
  - SCCP
- Provide advanced gateway functionality
  - DTMF relay
  - Supplementary services
- Work with redundant Cisco Unified Communication Manager
- Enable call survivability
- Provide QSIG support.
- Provide fax or modem services, or both

CVOICE v6.0—1-3

IP telephony gateways should meet these core feature requirements:

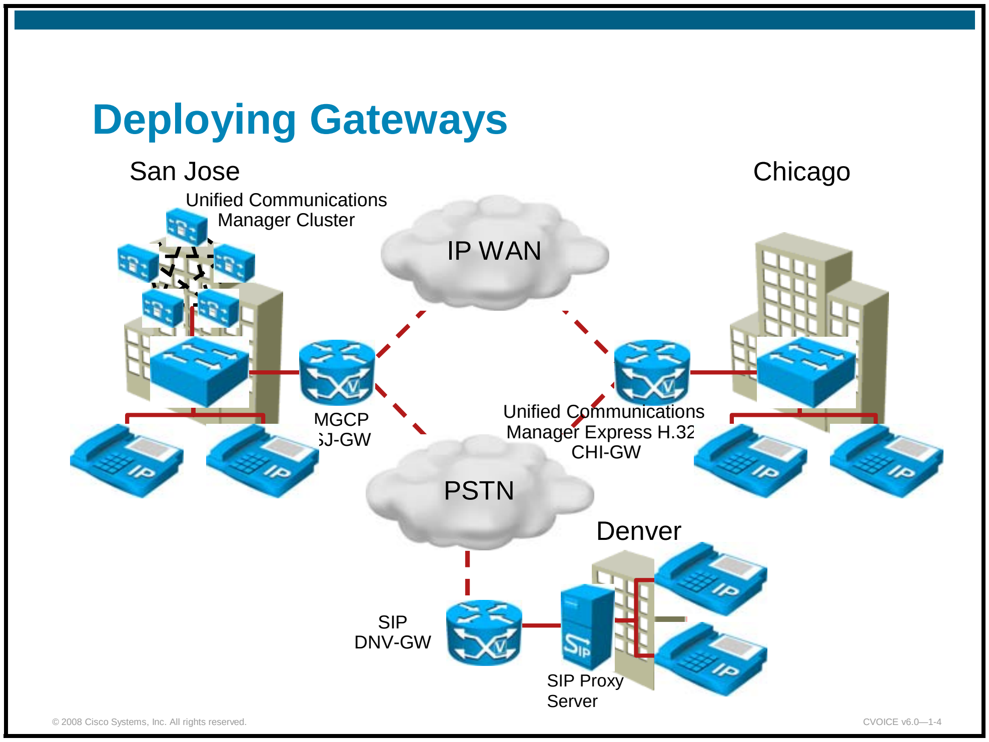
- **Gateway protocol support:** Cisco voice gateways support various signaling protocols, depending on the hardware platform. Cisco gateways support H.323, Media Gateway Control Protocol (MGCP), session initiation protocol (SIP), and Skinny Client Control Protocol (SCCP). H.323 and SIP gateways do not need a call control agent. Therefore, they can be deployed on networks in which call agents, such as Cisco Unified Communications Manager, are not present. MGCP and SCCP are streamlined protocols that only work on a network in which a call agent, such as a Cisco Unified Communications Manager, is present. Cisco IP phones use SCCP, which is a lighter-weight protocol. SCCP uses a client/server model, while H.323 is a peer-to-peer model. MGCP also follows a client/server model.

Protocol Selection

Protocol selection depends on site-specific requirements and the installed base of equipment. For example, many remote branch locations have Cisco 2600XM Series Multiservice Routers or Cisco 3700 Series Multiservice Access Routers installed. These routers support H.323 and MGCP 0.1 with Cisco IOS Release 12.2(11)T and Cisco Unified Communications Manager Release 3.1 or later. For gateway configuration, you might prefer MGCP to H.323 because of its simpler configuration. This option also works well with older Cisco IOS versions because it provides support for call survivability during a Cisco Unified Communications Manager failover from a primary to a secondary Cisco Unified Communications Manager. On the other hand, you might prefer H.323 over MGCP because of the more advanced interfaces supported.

The Simplified Message Desk Interface (SMDI) is a standard for integrating voice-mail systems to PBXs or Centrex systems. Connecting to a voice-mail system via SMDI using either analog FXS or digital T1 PRI requires either SCCP or MGCP because H.323 devices do not identify the specific line that is being used by a group of ports. The use of H.323 gateways for this purpose means the Cisco Messaging Interface cannot correctly correlate the SMDI information with the actual port or channel that is being used for an incoming call.

- **Advanced gateway functionality, of which there are two advanced features:**
  - **Dual tone multifrequency (DTMF) relay capabilities:** Each digit that is dialed with tone dialing is assigned a unique pair of frequencies. Voice compression of these tones with a low bit-rate coder-decoder (codec) can cause DTMF signal loss or distortion. Therefore, DTMF tones are separated from the voice bearer stream and sent as signaling indications through the gateway protocol (H.323, SCCP, or MGCP) signaling channel instead.
  - **Supplementary services support:** These services provide user functions such as hold, transfer, and conferencing, and are considered to be fundamental requirements of any voice installation.
- **Redundant Cisco Unified Communications Manager systems support:** The gateways must support the ability to "rehome" to a secondary Cisco Unified Communications Manager in the event of a primary Cisco Unified Communications Manager failure.
- **Call survivability in Cisco Unified Communications Manager:** The voice gateway preserves the Real-Time Transport Protocol (RTP) bearer stream (the voice conversation) between two IP endpoints when the Cisco Unified Communications Manager to which the endpoint is registered is no longer accessible.
- **Q Signaling (QSIG) support:** QSIG is becoming the standard for PBX interoperability in Europe and North America. With QSIG, the Cisco voice packet network appears to PBXs as a distributed transit PBX that can establish calls to any PBX or other telephony endpoint served by a Cisco gateway, including non-QSIG endpoints.
- **Fax and modem support:** Fax over IP enables interoperability of traditional analog fax machines with IP telephony networks. The fax image is converted from an analog signal and is transmitted as digital data over the packet network.



Deploying Gateways

CVOICE v6.0—1-4

Gateways are usually deployed as edge devices on a network. Because they will interface with both the PSTN and the company WAN, they must have the appropriate hardware and utilize the appropriate protocol for that network. The figure represents a scenario in which three different types of gateways are deployed for VoIP and PSTN interconnections.

The scenario displays the unified communications network of a company that was recently formed as a result of a merger of three individual companies. In the past, each company had its own strategy in terms of how they connected to the PSTN.

- The San Jose location used a Cisco Unified Communications Manager environment with a MGCP-controlled unified communications gateway to connect to the PSTN.
- The Chicago location used a Cisco Unified Communications Manager Express environment with an H.323-based unified communications gateway to connect to the PSTN.
- The Denver location used a Cisco SIP proxy server and SIP IP phones as well as a SIP-based unified communications gateway to connect to the PSTN. Because the Denver location is a small office, it does not use the WAN for IP telephony traffic to the other locations. Therefore, its local VoIP network is connected only to the PSTN.

Gateway Hardware Platforms

This topic describes the different Cisco gateway platforms.

Gateway Hardware Platforms

Modern enterprise models:

Cisco 2800 Series Routers

Cisco 3800 Series Routers

Cisco Catalyst 6500 Series

CVOICE v6.0—1-5

This figure depicts some of the modern enterprise models that are usually used within enterprise networks.

Modern Enterprise Models

Following are some of the current Cisco voice gateway models used in modern enterprise environments.

Cisco 2800 Series Integrated Services Routers

Cisco 2800 Series Integrated Services Routers comprise four models: Cisco 2801, Cisco 2811, Cisco 2821, and Cisco 2851 routers. The 2800 Series routers provide up to 5 times the overall performance, up to 10 times the security and voice performance, embedded service options, and dramatically increased slot performance and density. The series also maintains support for most of the more than 90 modules that are available for the Cisco 1700 Series Modular Access Routers, 2600 Series Multiservice Platforms, and 3700 Series Multiservice Access Routers

The 2800 Series routers can deliver simultaneous, high-quality, wire-speed services up to multiple T1/E1or xDSL connections. The routers offer embedded encryption acceleration and, on the motherboard, voice digital signal processor (DSP) slots. They also offer intrusion prevention system (IPS) and firewall functions; optional integrated call processing and voice-mail support; high-density interfaces for a wide range of wired and wireless connectivity requirements; and sufficient performance and slot density for future network expansion requirements and advanced applications.

Go to http://www.cisco.com/go/2800 to learn more about the Cisco 2800 Series routers.

Cisco 3800 Series Integrated Services Routers

Cisco 3800 Series Integrated Services Routers also feature embedded security processing, significant performance and memory enhancements, and new high-density interfaces that deliver the performance, availability, and reliability that are required to scale mission-critical security, IP telephony, business video, network analysis, and Web applications in the most demanding enterprise environments. The 3800 Series routers deliver multiple concurrent services at wire-speed T3/E3 rates.

The integrated services routing architecture of the 3800 Series routers is based on that of the 3700 Series routers. The routers are designed to embed and integrate security and voice processing with advanced wired and wireless services for rapid deployment of new applications, including application layer functions, intelligent network services, and converged communications. The 3800 Series routers support the bandwidth requirements for multiple Fast Ethernet interfaces per slot, TDM interconnections, and fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE). It also supports the existing portfolio of modular interfaces. This accommodates network expansion or changes in technology as new services and applications are deployed. By integrating the functions of multiple separate devices into a single compact unit, the 3800 Series reduces the cost and complexity of managing remote networks.

New 3800 Series models include the Cisco 3825 Integrated Services Router and the Cisco 3845 Integrated Services Router, available with three optional configurations for AC power, AC power with integrated inline power support, and DC power.

Go to http://www.cisco.com/go/3800 to learn more about the 3800 Series routers.

Cisco Catalyst 6500 Series Switches

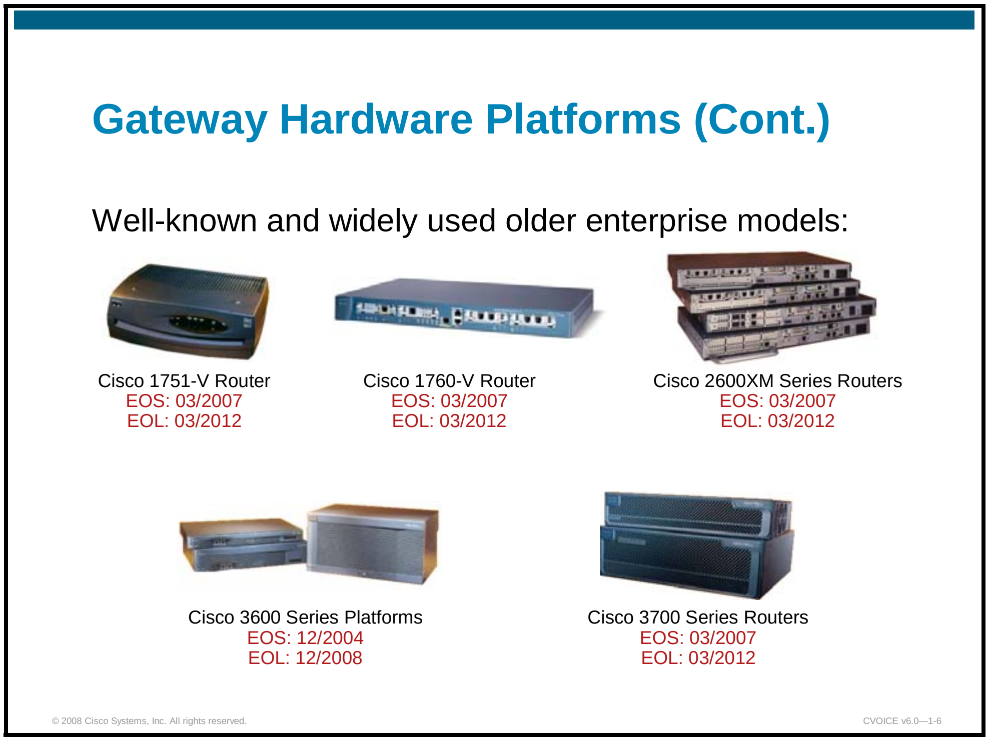
The Cisco Catalyst 6500 Series Switches are high-performance and feature-rich platforms that can be used as voice gateways by installing a Cisco Communication Media Module (CMM).

The Cisco CMM is a Cisco Catalyst 6500 Series line card that provides flexible and high-density VoIP gateway and media services. Catalyst 6500 Series Switches can handle many digital trunk interfaces. For example, Cisco Catalyst 6509 Switches support up to 144 T1/E1 connections by using eight communications media modules with 18 ports each. These gateway and media services allow organizations to connect their existing TDM network to their IP communications network, provide connectivity to the PSTN, and enable conferencing and transcoding services.

Go to http://www.cisco.com/go/catalyst6500 to learn more about Catalyst 6500 Series Switches.

Well-Known and Widely Used Enterprise Models

This figure shows some well-known and widely used enterprise models that have been in use for some time.



Gateway Hardware Platforms (Cont.)

Well-known and widely used older enterprise models:

Cisco 1751-V Router
EOS: 03/2007
EOL: 03/2012

Cisco 1760-V Router
EOS: 03/2007
EOL: 03/2012

Cisco 2600XM Series Routers
EOS: 03/2007
EOL: 03/2012

Cisco 3600 Series Platforms
EOS: 12/2004
EOL: 12/2008

Cisco 3700 Series Routers
EOS: 03/2007
EOL: 03/2012

CVOICE v6.0—1-6

The figure summarizes the enterprise models of Cisco modular access routers that have voice gateway capabilities. These models are well-known and widely used, and although they are announced to reach end of sale (EOS)—or, in the case of the Cisco 2600 Series, are already EOS—you need to know and support these models. Because they were the leading voice gateway products for a long time, nearly all Cisco customers have one or more of these systems on the network.

Cisco 1751-V Modular Access Router

The Cisco 1751-V Modular Access Router supports multiservice integration of voice, video, data, and fax traffic. The router offers many WAN-access and voice-interface options, VoIP, high-performance routing with bandwidth management, inter-virtual LAN routing, and virtual private network (VPN) access with a firewall.

Cisco 1760-V Modular Access Router

The Cisco 1760-V Modular Access Router offers small-to-medium-sized businesses and small enterprise branch offices a 19-inch rack-mount access solution designed to take advantage of the productivity of business applications. The router ensures the multiservice integration of voice, video, data, and fax traffic. It provides businesses with the complete functionality and flexibility to deliver secure Internet and intranet access. The router has many WAN access options, VoIP, high-performance routing with quality of service (QoS), intervirtual LAN routing, and VPN access with firewall options. Powered by Cisco IOS software, the Cisco 1760-V Modular Access Router allows simplified management and traffic prioritization, ensuring that business and time-sensitive applications perform as expected.

Go to http://www.cisco.com/go/1700 to learn more about the Cisco 1700 Series Modular Access Routers.

Cisco 2600XM Series Multiservice Routers

The modular architecture of the Cisco 2600XM Series Multiservice Routers enables you to upgrade interfaces to accommodate network expansion or changes in technology as new services and applications are deployed. Modular interfaces are shared with the Cisco 1700 Series Modular Access Routers and the Cisco 3700 Series Multiservice Access Routers, providing investment protection and reducing the complexity of managing the remote network solution by integrating the functions of multiple, separate devices into a single, compact unit. Network modules that are available for 2600XM Series and 3700 Series routers support many applications, including multiservice voice and data integration, integrated switching, analog and ISDN dial access, and serial device concentration.

Go to http://www.cisco.com/go/2600 to learn more about the Cisco 2600XM Series Multiservice Routers.

Cisco 3600 Series Multiservice Platforms

Cisco 3600 Series platforms are a family of modular, multiservice access platforms for medium- and large-sized offices and smaller Internet service providers (ISPs). With more than 70 modular interface options, Cisco 3600 Series platforms provide solutions for data, voice, video, hybrid dial access, VPNs, and multiprotocol data routing. The high-performance, modular architecture protects customer investments in network technology and integrates the functions of several devices within a single, manageable solution.

Cisco extended the Cisco 3600 Series platforms with the Cisco 3660 Multiservice Platform. The Cisco 3660 platform provides higher densities, greater performance, and more expansion capabilities. The additional power and performance of the Cisco 3660 platform enables new applications, such as packetized voice aggregation and branch office ATM access ranging from T1/E1 Inverse Multiplexing over ATM (IMA) to Optical Carrier 3 (OC-3).

Go to http://www.cisco.com/go/3600 to learn more about the Cisco 3600 Series Multiservice Platforms.

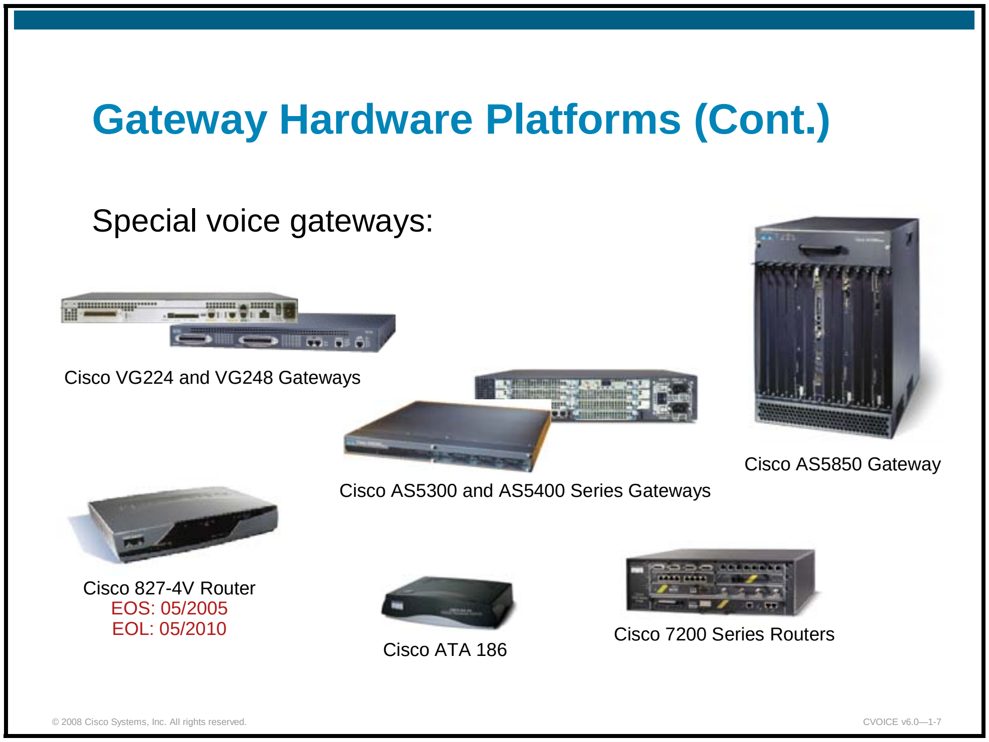
Cisco 3700 Series Multiservice Access Routers

The Cisco 3700 Series Multiservice Access Routers are modular routers that enable flexible and scalable deployment of e-business applications for the Cisco full-service branch (FSB) office. The 3700 Series Multiservice Access Routers optimize the branch office with high-performance routing, integrated low-density switching, security, voice, IP telephony, voice mail, video, and content networking in an integrated solution. This integrated design enables enterprise customers to adapt to evolving business needs by enhancing Cisco IOS services, such as QoS, IP multicast, VPN, Cisco IOS firewall, and an IPS. The 3700 Series Multiservice Access Routers are based on the same modular concepts as the 3600 Series platforms, but they enable higher levels of performance and service integration for the branch office.

Go to http://www.cisco.com/go/3700 to learn more about the Cisco 3700 Series Multiservice Access Routers.

Standalone Voice Gateways

This figure shows some standalone gateway models.



Gateway Hardware Platforms (Cont.)

Special voice gateways:

Cisco VG224 and VG248 Gateways

Cisco AS5300 and AS5400 Series Gateways

Cisco AS5850 Gateway

Cisco 827-4V Router
EOS: 05/2005
EOL: 05/2010

Cisco ATA 186

Cisco 7200 Series Routers

CVOICE v6.0—1-7

To fit special needs within the customer unified messaging system, Cisco offers standalone voice gateways for specific purposes. Each of these voice gateways fulfills a different need, such as the integration of analog devices into the unified messaging system, enhanced performance, business-class functionality, adaptability, serviceability, and manageability.

Cisco VG224 and VG248 Analog Phone Gateways

Cisco VG200 Series Gateways—including Cisco VG224 Analog Phone Gateway and Cisco VG248 Analog Phone Gateway—provide support for traditional analog devices while taking advantage of the new capabilities that Cisco Unified Communications affords.

Cisco VG200 Series Gateways include these features:

- VG200 Series Gateways are high-density gateways for using analog phones, fax machines, modems, voice-mail systems, and speakerphones.
- VG200 Series Gateways offer feature-rich functionality for enterprise voice systems based on Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.
- The VG224 Analog Phone Gateway is based on a Cisco IOS software platform and offers 24 fully featured analog ports for use as extensions to Cisco Unified Communications Manager or Cisco Unified Communications Manager Express systems in a compact 19-inch rack-mount chassis.
- The VG248 Analog Phone Gateway offers 48 fully featured analog ports for use as extensions to the Cisco Unified Communications Manager system in a compact 19-inch rack-mount chassis.

Cisco AS5300 Series Universal Gateways

The Cisco AS5300 Series gateways include the Cisco AS5350 Universal Gateway and the Cisco AS5350XM Universal Gateway. The AS5350XM Universal Gateway doubles the performance of the Cisco AS5350 Universal Gateway, allowing the same applications to run faster and with lower CPU utilization levels.

Go to http://www.cisco.com/go/as5300 to learn more about the Cisco AS5300 Series Universal Gateways.

Cisco AS5400 Series Universal Gateways

The Cisco AS5400 Series gateways include the Cisco AS5400HPX Universal Gateway, which enhances performance for processor-intensive voice and fax applications, and the Cisco AS5400XM Universal Gateway. These gateway models double the performance of the Cisco AS5400 Universal Gateway and AS5400HPX Universal Gateway models and allow the same applications to run faster and with lower CPU utilization levels.

Go to http://www.cisco.com/go/as5400 to learn more about the Cisco AS5400 Series Universal Gateways.

Cisco AS5850 Universal Gateway

The Cisco AS5850 Universal Gateway is a high-density, carrier-class gateway with high capacity and availability. The AS5850 Universal Gateway is specifically designed to meet the demands of large service providers by supporting up to 5 channelized T3s (CT3s), 96 T1s, or 86 E1s of data, voice, and fax services, on any port at any time. It offers high-availability features such as hot swap on all cards, load-sharing and redundant hot-swappable power supplies, redundant route-processing cards, and Call Admission Control (CAC) to ensure 99.999 percent availability.

Go to http://www.cisco.com/go/as5850 to learn more about the Cisco AS5850 Universal Gateway.

Cisco 827-4V ADSL Router

The Cisco 827-4V ADSL Router provides business-class functionality for small businesses, small remote offices, and corporate teleworkers using Cisco IOS technology. It enables service providers and resellers to increase service revenue by supporting features for business-class security, integrated toll-quality voice and data, differentiated service classes, and managed network access. These features, along with the manageability and reliability of Cisco IOS software, provide mission-critical networking.

With the software upgradeable platform of the 827-4V ADSL Router, service providers and resellers can increase revenue by offering DSL services today and provide value-added services as the technology needs of their customers grow. The Cisco 827-4V ADSL Router is one of the Cisco 800 Series Routers.

Go to http://www.cisco.com/go/800 to learn more about the Cisco 800 Series Routers.

Cisco ATA 186

The Cisco Analog Telephone Adaptor 186 (ATA 186) is a handset-to-Ethernet adapter that allows traditional telephone devices to function as VoIP devices. Customers can use IP telephony applications by connecting their analog devices to analog telephone adapters.

The ATA 186 supports two voice ports, which each have an independent telephone number and a single 10BASE-T Ethernet port. This adaptor can make use of existing Ethernet LANs, in addition to broadband pipes such as DSL, fixed wireless, and cable modem deployments.

The Cisco ATA 180 Series products are standards-based IP communications devices that deliver VoIP terminations to businesses and residences.

Go to http://www.cisco.com/go/ata186 to learn more about the Cisco ATA 186.

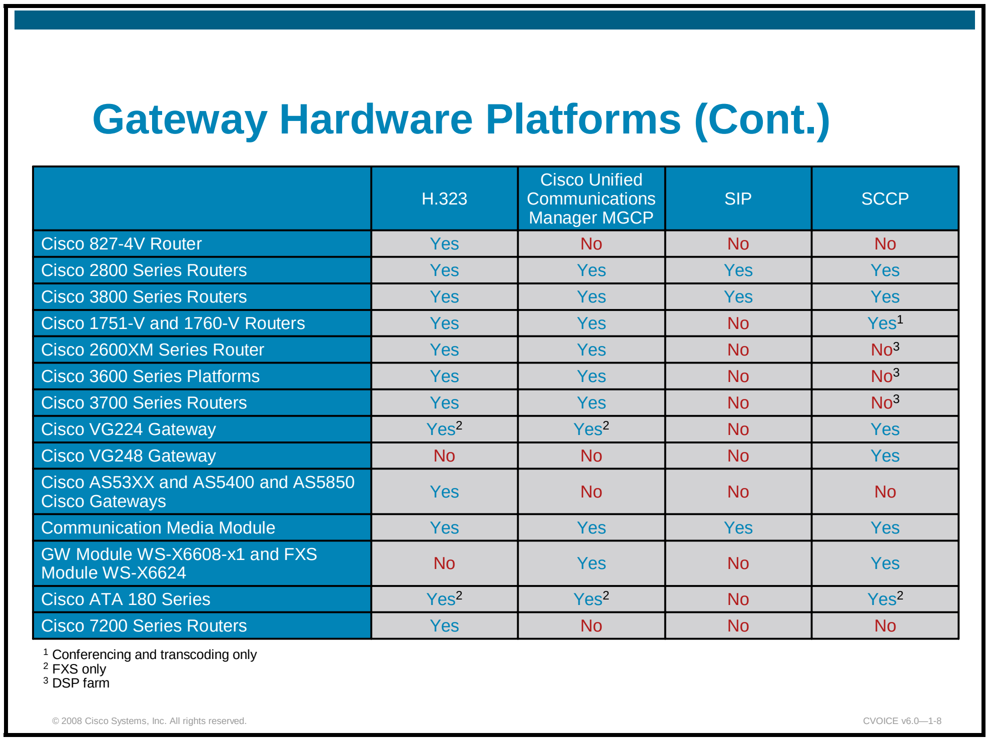
Cisco 7200 Series Routers

Cisco 7200 Series Routers are services routers for enterprise edge and service provider edge applications. These compact routers provide serviceability and manageability coupled with high-performance modular processors such as the Cisco 7200 Series NPE-G1 Network Processing Engine.

Go to http://www.cisco.com/go/7200 to learn more about the Cisco 7200 Series Routers.

Summary of Voice Gateways

This subtopic summarizes the Cisco voice gateway platforms and provides a short overview of their usage.



Gateway Hardware Platforms (Cont.)

	H.323	Cisco Unified Communications Manager MGCP	SIP	SCCP
Cisco 827-4V Router	Yes	No	No	No
Cisco 2800 Series Routers	Yes	Yes	Yes	Yes
Cisco 3800 Series Routers	Yes	Yes	Yes	Yes
Cisco 1751-V and 1760-V Routers	Yes	Yes	No	Yes[1]
Cisco 2600XM Series Router	Yes	Yes	No	No[3]
Cisco 3600 Series Platforms	Yes	Yes	No	No[3]
Cisco 3700 Series Routers	Yes	Yes	No	No[3]
Cisco VG224 Gateway	Yes[2]	Yes[2]	No	Yes
Cisco VG248 Gateway	No	No	No	Yes
Cisco AS53XX and AS5400 and AS5850 Cisco Gateways	Yes	No	No	No
Communication Media Module	Yes	Yes	Yes	Yes
GW Module WS-X6608-x1 and FXS Module WS-X6624	No	Yes	No	Yes
Cisco ATA 180 Series	Yes[2]	Yes[2]	No	Yes[2]
Cisco 7200 Series Routers	Yes	No	No	No

[1] Conferencing and transcoding only
[2] FXS only
[3] DSP farm

CVOICE v6.0—1-8

The table above summarizes the Cisco voice gateway platforms.

The table below provides a short overview of their uses.

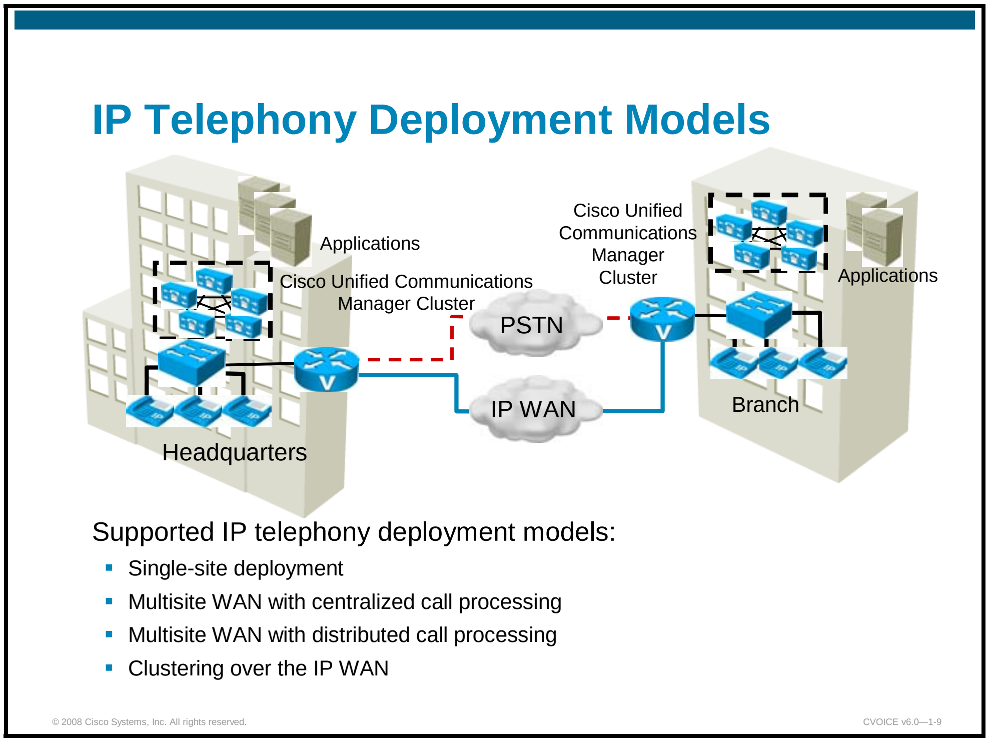
Gateway Hardware Platforms

Device/Series	Use
Cisco 827-4V router	Connects up to four analog devices via ADSL
Cisco 2800 Series routers	Used for small-to-medium-sized enterprise voice gateways
Cisco 3800 Series routers	Used for large-sized enterprise voice gateways
Cisco 1751-V and 1760-V routers	Used for small-sized enterprise voice gateways
Cisco 2600XM Series routers	Used for medium-sized enterprise voice gateways
Cisco 3600 Series platforms	Used for medium-sized enterprise voice gateways
Cisco 3700 Series routers	Used for large-sized enterprise voice gateways
Cisco VG224 gateway	Connects up to 24 analog devices to the VoIP network
Cisco VG248 gateway	Connects up to 48 analog devices to the VoIP network
Cisco AS5350, AS5350XM, AS5400HPX, AS5400XM, and AS5850 gateways	Is a service provider voice gateway
Cisco Communications Media Module	Provides T1/E1 and FXS interfaces and conferencing and transcoding resources on Cisco Catalyst 6500 Series Switches

Device/Series	Use
Cisco Catalyst 6000 WS-X6608-E1 and Catalyst 6000 WS-X6608-T1 gateway modules and Cisco Catalyst 6000 WS-X6624-FXS	Provides T1/E1 and FXS interfaces on Catalyst 6500 Series Switches
Cisco ATA 186	Connects up to two analog devices to the VoIP network
Cisco 7200 Series routers	Is a service provider voice gateway

IP Telephony Deployment Models

This topic describes supported IP telephony deployment models.



IP Telephony Deployment Models

Applications
Cisco Unified Communications Manager Cluster
Cisco Unified Communications Manager Cluster
Applications
PSTN
IP WAN
Headquarters
Branch

Supported IP telephony deployment models:

- Single-site deployment
- Multisite WAN with centralized call processing
- Multisite WAN with distributed call processing
- Clustering over the IP WAN

© 2008 Cisco Systems, Inc. All rights reserved.

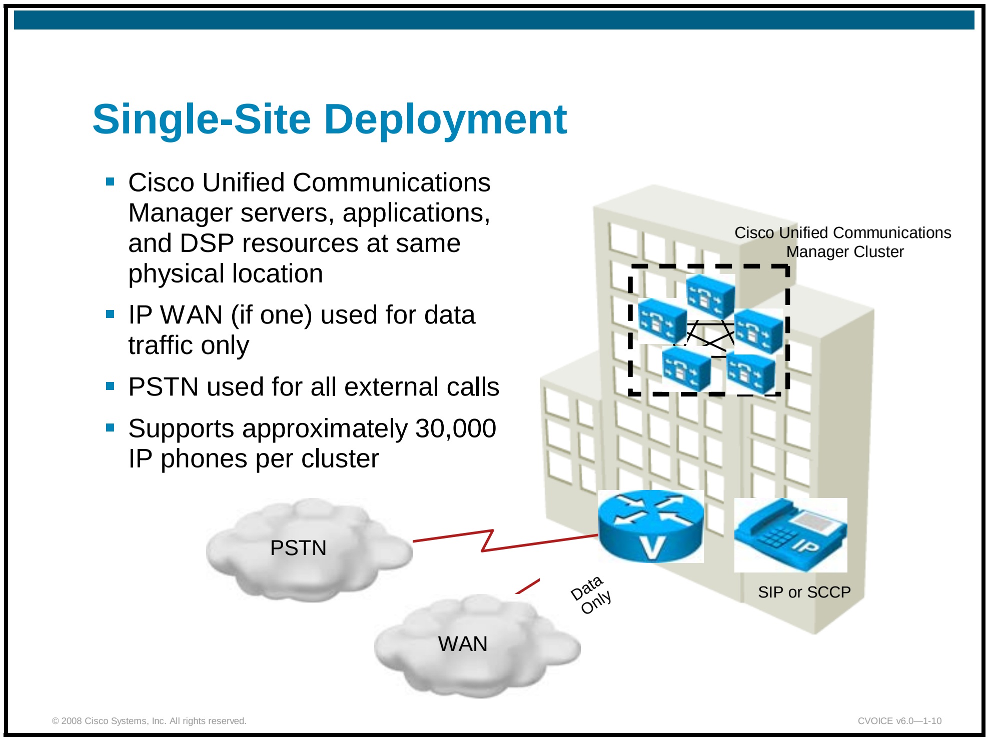
CVOICE v6.0—1-9

Each deployment model differs in the type of traffic that is carried over the WAN, the location of the call-processing agent, and the size of the deployment. Cisco IP telephony supports these deployment models:

- Single-site
- Multisite with centralized call processing
- Multisite with distributed call processing
- Clustering over the IP WAN

Single-Site Deployment

This topic describes the major characteristics and design guidelines of a single-site IP telephony deployment model.



Single-Site Deployment

- Cisco Unified Communications Manager servers, applications, and DSP resources at same physical location
- IP WAN (if one) used for data traffic only
- PSTN used for all external calls
- Supports approximately 30,000 IP phones per cluster

CVOICE v6.0—1-10

The single-site model for Cisco Unified Communications consists of a call-processing agent cluster located at a single site, or campus, with no telephony services provided over an IP WAN. All Cisco Unified Communications Manager servers, applications, and DSP resources are located in the same physical location. You can implement multiple clusters inside a LAN or a metropolitan-area network (MAN) and connect them through intercluster trunks if you need to deploy more IP phones in a single-site configuration.

An enterprise would typically deploy the single-site model over a LAN or MAN, which carries the voice traffic within the site. Gateway trunks that connect directly to the PSTN handle all external calls. If an IP WAN exists between sites, it is used to carry data traffic only; no telephony services are provided over the WAN.

Design Characteristics

The single-site model has the following design characteristics:

- Single Cisco Unified Communications Manager cluster.
- Maximum of 30,000 SCCP or SIP IP phones or SCCP video endpoints per cluster.
- Maximum of 1100 H.323 devices (gateways, multipoint control units, trunks, and clients) or MGCP gateways per Cisco Unified Communications Manager cluster.
- PSTN for all calls outside the site.
- DSP resources for conferencing, transcoding, and Media Termination Point (MTP).
- Voice mail, unified messaging, Cisco Unified Presence, and audio and video components.

- Capability to integrate with legacy PBX and voice-mail systems.
- H.323 clients, multipoint control units, and H.323/H.320 gateways that require a gatekeeper to place calls must register with a Cisco IOS gatekeeper (Cisco IOS Release 12.3(8)T or later). Cisco Unified Communications Manager then uses an H.323 trunk to integrate with the gatekeeper and provide call routing and bandwidth management services for the H.323 devices that are registered to it. Multiple Cisco IOS gatekeepers may be used to provide redundancy.
- Multipoint control unit resources are required for multipoint video conferencing. Depending on conferencing requirements, these resources may be either SCCP or H.323, or both.
- H.323/H.320 video gateways are needed to communicate with H.320 videoconferencing devices on the public ISDN network.
- High-bandwidth audio (for example, G.711, G.722, or Cisco wideband audio) between devices within the site.
- High-bandwidth video (for example, 384 kb/s or higher) between devices within the site. The Cisco Unified Video Advantage wideband codec, operating at 7 Mb/s, is also supported.

Benefits of the Single-Site Model

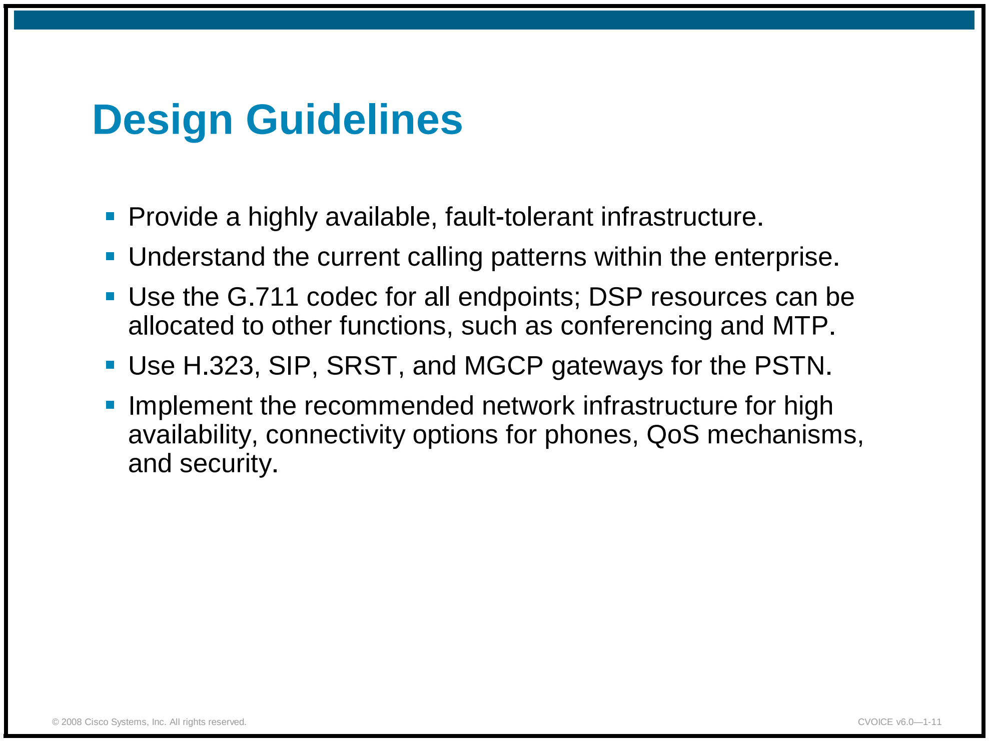
A single infrastructure for a converged network solution provides significant cost benefits and enables Cisco Unified Communications to take advantage of the many IP-based applications in the enterprise. Single-site deployment also allows each site to be completely self-contained. There is no dependency for service in the event of an IP WAN failure or insufficient bandwidth, and there is no loss of call-processing service or functionality.

The main benefits of the single-site model are:

- Ease of deployment
- A common infrastructure for a converged solution
- Simplified dial plan
- No required transcoding resources, due to the use of only a single high-bandwidth codec

Single-Site Deployment: Design Guidelines

This subtopic covers single-site design guidelines and best practices.



Design Guidelines

- Provide a highly available, fault-tolerant infrastructure.
- Understand the current calling patterns within the enterprise.
- Use the G.711 codec for all endpoints; DSP resources can be allocated to other functions, such as conferencing and MTP.
- Use H.323, SIP, SRST, and MGCP gateways for the PSTN.
- Implement the recommended network infrastructure for high availability, connectivity options for phones, QoS mechanisms, and security.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-11

Single-site deployment is a subset of the distributed and centralized call-processing model. Future scalability requires that you adhere to the recommended best practices specific to the distributed and centralized call-processing model. When you develop a stable, single site that is based on a common infrastructure philosophy, you can easily expand the IP telephony system applications, such as video streaming and videoconferencing, to remote sites.

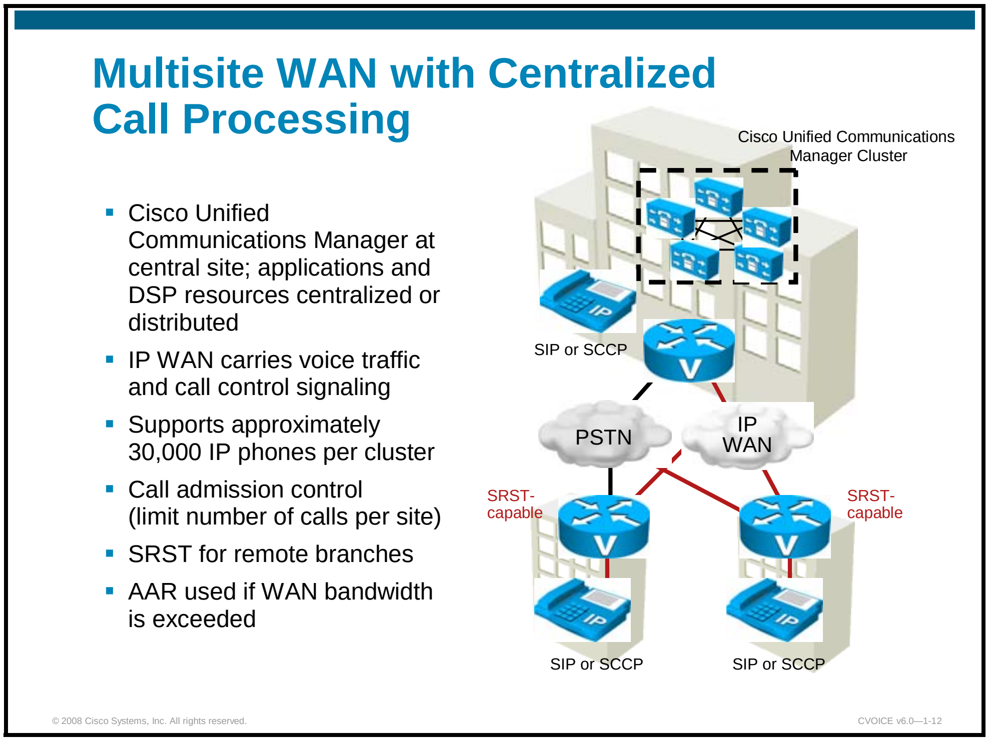
Best Practices

Follow these guidelines and best practices when implementing the single-site model:

- Provide a highly available, fault-tolerant infrastructure based on a common infrastructure philosophy. A sound infrastructure is essential for easier migration to Cisco Unified Communications, integration with applications such as video streaming and video conferencing, and expansion of your Cisco Unified Communications deployment across the WAN or to multiple Cisco Unified Communications Manager clusters.
- Know the calling patterns for your enterprise. Use the single-site model if most of the calls from your enterprise are within the same site or to PSTN users outside your enterprise.
- Use G.711 codecs for all endpoints. This practice eliminates the consumption of DSP resources for transcoding, and those resources can be allocated to other functions such as conferencing and MTPs.
- Use SIP, SRST, and MGCP gateways for the PSTN. This practice simplifies the dial plan configuration. H.323 might be required to support specific functionality such as Signaling System 7 (SS7) or Non-Facility Associated Signaling (NFAS).
- Implement the recommended network infrastructure for high availability, connectivity options for phones (in-line power), QoS mechanisms, and security.

Multisite WAN with Centralized Call Processing

This topic describes the major characteristics and design guidelines of a multisite centralized IP telephony deployment model.



Multisite WAN with Centralized Call Processing

- Cisco Unified Communications Manager at central site; applications and DSP resources centralized or distributed
- IP WAN carries voice traffic and call control signaling
- Supports approximately 30,000 IP phones per cluster
- Call admission control (limit number of calls per site)
- SRST for remote branches
- AAR used if WAN bandwidth is exceeded

CVOICE v6.0—1-12

The model for a multisite WAN deployment with centralized call processing consists of a single call-processing agent cluster that provides services for many remote sites and uses the IP WAN to transport Cisco Unified Communications traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites. The figure illustrates a typical centralized call-processing deployment, with a Cisco Unified Communications Manager cluster as the call-processing agent at the central site and an IP WAN with QoS enabled to connect all the sites. The remote sites rely on the centralized Cisco Unified Communications Manager cluster to handle their call processing. Applications such as voice mail, presence servers, IVR systems, and so forth, are typically also centralized to reduce the overall costs of administration and maintenance.

The WAN connectivity options include the following:

- Leased lines
- Frame Relay
- ATM
- ATM and Frame Relay service interworking (SIW)
- Multiprotocol Label Switching (MPLS) VPN
- Voice and Video Enabled VPN (V3PN) IP Security (IPsec) protocol

Routers that reside at the WAN edges require QoS mechanisms, such as priority queuing and traffic shaping, to protect the voice traffic from the data traffic across the WAN, where bandwidth is typically scarce. In addition, a CAC scheme is needed to avoid oversubscribing the WAN links with voice traffic and deteriorating the quality of established calls. For centralized call-processing deployments, the locations construct within Cisco Unified Communications Manager provides CAC.

A variety of Cisco gateways can provide the remote sites with PSTN access. When the IP WAN is down, or if all the available bandwidth on the IP WAN has been consumed, users at the remote sites can dial the PSTN access code and place their calls through the PSTN. The Cisco Unified Survivable Remote Site Telephony (SRST) feature, available for both SCCP and SIP phones, provides call processing at the branch offices for Cisco Unified IP phones if they lose their connection to the remote primary, secondary, or tertiary Cisco Unified Communications Manager or if the WAN connection is down. Cisco Unified SRST functionality is available on Cisco IOS gateways running the SRST feature or on Cisco Unified Communications Manager Express Release 4.0 and higher running in SRST mode. Cisco Unified Communications Manager Express running in SRST mode provides more features for the phones than SRST on a Cisco IOS gateway does.

Design Characteristics

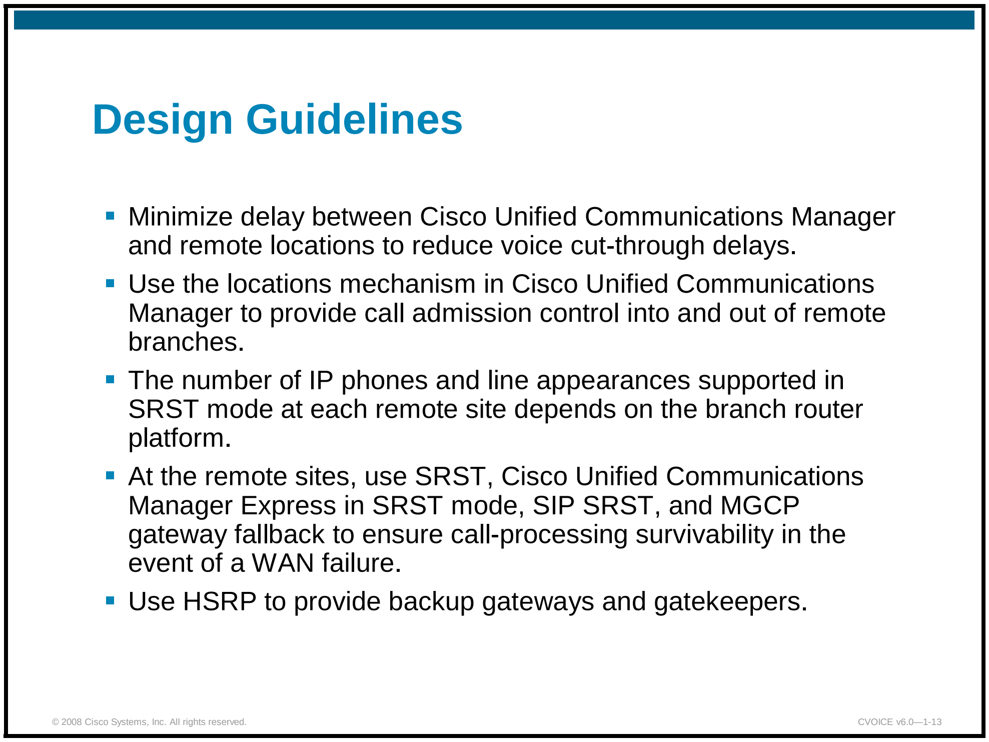
The multisite model with centralized call processing has the following design characteristics:

- Single Cisco Unified Communications Manager cluster.
- Maximum of 30,000 SCCP or SIP IP phones or SCCP video endpoints per cluster.
- Maximum of 1000 locations per Cisco Unified Communications Manager cluster.
- Maximum of 1100 H.323 devices (gateways, multipoint control units, trunks, and clients) or 1100 MGCP gateways per Cisco Unified Communications Manager cluster.
- PSTN for all external calls.
- DSP resources for conferencing, transcoding, and MTP.
- Voice mail, unified messaging, Cisco Unified Presence, and audio and video components.
- Capability to integrate with legacy PBX and voice-mail systems.
- H.323 clients, multipoint control units, and H.323/H.320 gateways that require a gatekeeper to place calls must register with a Cisco IOS gatekeeper (Cisco IOS Release 12.3(8)T or later). Cisco Unified Communications Manager then uses an H.323 trunk to integrate with the gatekeeper and provide call routing and bandwidth management services for the H.323 devices that are registered to it. Multiple Cisco IOS gatekeepers may be used to provide redundancy.
- Multipoint control unit resources are required for multipoint video conferencing. Depending on conferencing requirements, these resources may be either SCCP or H.323, or both, and may all be located at the central site or may be distributed to the remote sites if local conferencing resources are required.
- H.323/H.320 video gateways are needed to communicate with H.320 videoconferencing devices on the public ISDN network. These gateways may all be located at the central site or may be distributed to the remote sites if local ISDN access is required.
- High-bandwidth audio (for example, G.711, G.722, or Cisco wideband audio) between devices in the same site, and low-bandwidth audio (for example, G.729 or G.728) between devices in different sites.

- High-bandwidth video (for example, 384 kb/s or higher) between devices in the same site, and low-bandwidth video (for example, 128 kb/s) between devices at different sites. The Cisco Unified Video Advantage wideband codec, operating at 7 Mb/s, is recommended only for calls between devices at the same site.
- Minimum of 768 kb/s or higher WAN link speeds. Video is *not* recommended on WAN connections that operate at speeds lower than 768 kb/s.
- Cisco Unified Communications Manager locations provide CAC, and automated alternate routing (AAR) is also supported for video calls.
- SRST versions 4.0 and higher support video. However, versions of SRST prior to 4.0 do *not* support video, and SCCP video endpoints located at remote sites become audio-only devices if the WAN connection fails.
- Cisco Unified Communications Manager Express versions 4.0 and higher may be used instead of an SRST router for remote site survivability. Cisco Unified Communications Manager Express also provides more features than the SRST router does during WAN outage.
- Cisco Unified Communications Manager Express can be integrated with the Cisco Unity server in the branch office or remote site. The Cisco Unity server is registered to the Cisco Unified Communications Manager at the central site in normal mode and can fall back to Cisco Unified Communications Manager Express in SRST mode when Cisco Unified Communications Manager is not reachable, or during a WAN outage, to provide the users at the branch offices with access to their voice mail with Message Waiting Indicator (MWI).

Multisite WAN with Centralized Call Processing: Design Guidelines

This subtopic details the best-practice guidelines to follow when you are deploying a centralized IP telephony model.



Design Guidelines

- Minimize delay between Cisco Unified Communications Manager and remote locations to reduce voice cut-through delays.
- Use the locations mechanism in Cisco Unified Communications Manager to provide call admission control into and out of remote branches.
- The number of IP phones and line appearances supported in SRST mode at each remote site depends on the branch router platform.
- At the remote sites, use SRST, Cisco Unified Communications Manager Express in SRST mode, SIP SRST, and MGCP gateway fallback to ensure call-processing survivability in the event of a WAN failure.
- Use HSRP to provide backup gateways and gatekeepers.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-13

Follow these guidelines when you are implementing the multisite WAN model with centralized call processing:

- Minimize delay between Cisco Unified Communications Manager and remote locations to reduce voice cut-through delays (also known as clipping). Cisco recommends 150 ms maximum one way.
- Use the locations mechanism in Cisco Unified Communications Manager to provide CAC into and out of remote branches.
- The number of IP phones and line appearances that are supported in SRST mode at each remote site depends on the branch router platform, the amount of memory installed, and the Cisco IOS release. SRST on a Cisco IOS gateway supports up to 720 phones, while Cisco Unified Communications Manager Express running in SRST mode supports 240 phones. However, the choice of whether to adopt a centralized call-processing or distributed call-processing approach for a given site depends on a number of factors:
    - IP WAN bandwidth or delay limitations
    - Criticality of the voice network
    - Feature set needs
    - Scalability
    - Ease of management
    - Cost

Note If a distributed call-processing model is deemed more suitable for the customer business needs, the choices include installing a Cisco Unified Communications Manager cluster at each site or running Cisco Unified Communications Manager Express at the remote sites.

- At the remote sites, use the following features to ensure call processing survivability in the event of a WAN failure:
  - For SCCP phones, use SRST on a Cisco IOS gateway or Cisco Unified Communications Manager Express running in SRST mode.
  - For SIP phones, use SIP SRST.
  - For MGCP phones, use MGCP gateway fallback.

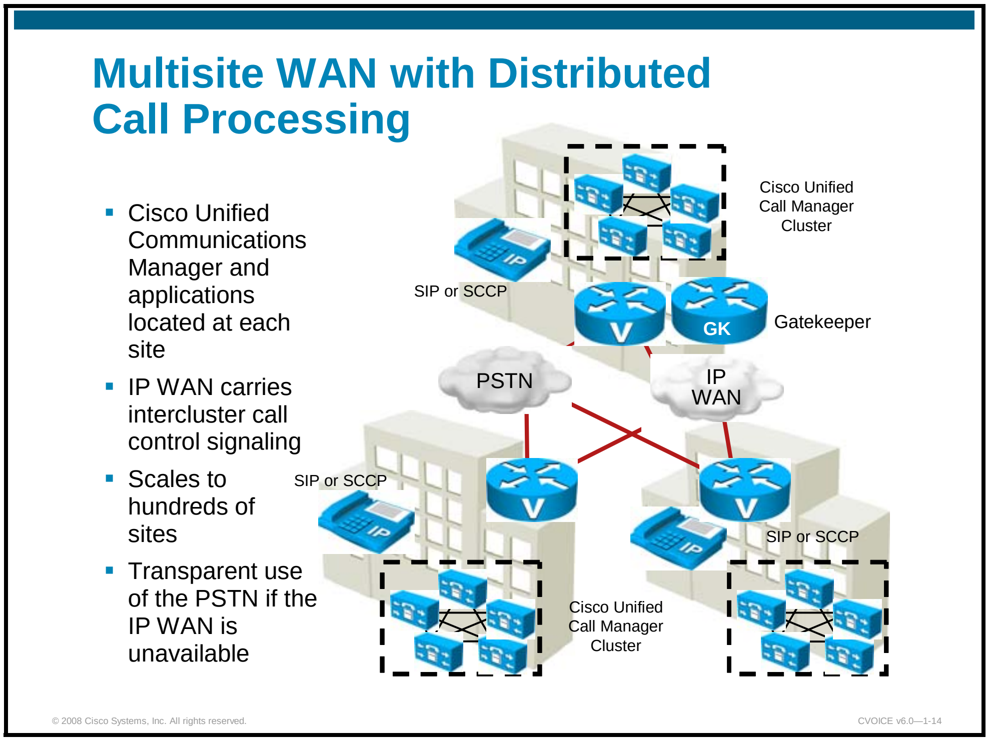
  SRST or Cisco Unified Communications Manager Express in SRST mode, SIP SRST, and MGCP gateway fallback can reside with each other on the same Cisco IOS gateway.

- Hot Standby Router Protocol (HSRP) may be used to provide backups for gateways and gatekeepers in a VoIP environment.

For specific sizing recommendations, refer to *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html.

Multisite WAN with Distributed Call Processing

This topic describes the major characteristics and design guidelines of a multisite distributed IP telephony deployment model.



Multisite WAN with Distributed Call Processing

- Cisco Unified Communications Manager and applications located at each site
- IP WAN carries intercluster call control signaling
- Scales to hundreds of sites
- Transparent use of the PSTN if the IP WAN is unavailable

Cisco Unified Call Manager Cluster
SIP or SCCP
IP
V
GK
Gatekeeper
PSTN
IP WAN
SIP or SCCP
IP
V
V
IP
SIP or SCCP
Cisco Unified Call Manager Cluster

© 2008 Cisco Systems, Inc. All rights reserved.　CVOICE v6.0—1-14

The model for a multisite WAN deployment with distributed call processing consists of multiple independent sites, each with its own call-processing agent cluster connected to an IP WAN that carries voice traffic between the distributed sites.

Depending on your network design, a distributed call-processing site may consist of any of the following:

- A single site with its own call-processing agent, which can be one of the following:
  - Cisco Unified Communications Manager
  - Cisco Unified Communications Manager Express
  - Other IP PBX
- A centralized call-processing site and all of its associated remote sites
- A legacy PBX with a VoIP gateway

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

The WAN connectivity options include the following:

- Leased lines
- Frame Relay

- ATM
- ATM and Frame Relay SIW
- MPLS VPN
- V3PN IPsec

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

Design Characteristics

The multisite model with distributed call processing has the following design characteristics:

- Maximum of 30,000 SCCP or SIP IP phones or SCCP video endpoints per cluster.
- Maximum of 1100 MGCP gateways or H.323 devices (gateways, multipoint control units, trunks, and clients) per Cisco Unified Communications Manager cluster.
- PSTN for all external calls.
- DSP resources for conferencing, transcoding, and MTP.
- Voice mail, unified messaging, and Cisco Unified Presence components.
- Capability to integrate with legacy PBX and voice-mail systems.
- H.323 clients, multipoint control units, and H.323/H.320 gateways that require a gatekeeper to place calls must register with a Cisco IOS gatekeeper (Cisco IOS Release 12.3(8)T or later). Cisco Unified Communications Manager then uses an H.323 trunk to integrate with the gatekeeper and provide call routing and bandwidth management services for the H.323 devices registered to it. Multiple Cisco IOS gatekeepers may be used to provide redundancy. Cisco IOS gatekeepers may also be used to provide call routing and bandwidth management between the distributed Cisco Unified Communications Manager clusters. In most situations, Cisco recommends that each Cisco Unified Communications Manager cluster have its own set of endpoint gatekeepers and that a separate set of gatekeepers be used to manage the intercluster calls. In some circumstances, it is possible to use the same set of gatekeepers for both functions, depending on the size of the network, complexity of the dial plan, and so forth.
- Multipoint control unit resources are required in each cluster for multipoint video conferencing. Depending on conferencing requirements, these resources may be either SCCP or H.323, or both, and may all be located at the regional sites or may be distributed to the remote sites of each cluster if local conferencing resources are required.
- H.323/H.320 video gateways are needed to communicate with H.320 videoconferencing devices on the public ISDN network. These gateways may all be located at the regional sites or may be distributed to the remote sites of each cluster if local ISDN access is required.
- High-bandwidth audio (for example, G.711, G.722, or Cisco wideband audio) between devices in the same site, but low-bandwidth audio (for example, G.729 or G.728) between devices in different sites.

- High-bandwidth video (for example, 384 kb/s or higher) between devices in the same site, but low-bandwidth video (for example, 128 kb/s) between devices at different sites. The Cisco Unified Video Advantage wideband codec, operating at 7 Mb/s, is recommended only for calls between devices at the same site. Note that the Cisco Video Telephony (VT) Camera wideband video codec is not supported over intercluster trunks.
- Minimum of 768 kb/s or higher WAN link speeds. Video is not recommended on WAN connections that operate at speeds lower than 768 kb/s.
- CAC is provided by Cisco Unified Communications Manager locations for calls between sites controlled by the same Cisco Unified Communications Manager cluster, and by the Cisco IOS gatekeeper for calls between Cisco Unified Communications Manager clusters (that is, intercluster trunks). AAR is also supported for both intracluster and intercluster video calls.

Benefits

The main benefits of the multisite WAN with distributed call-processing deployment model are as follows:

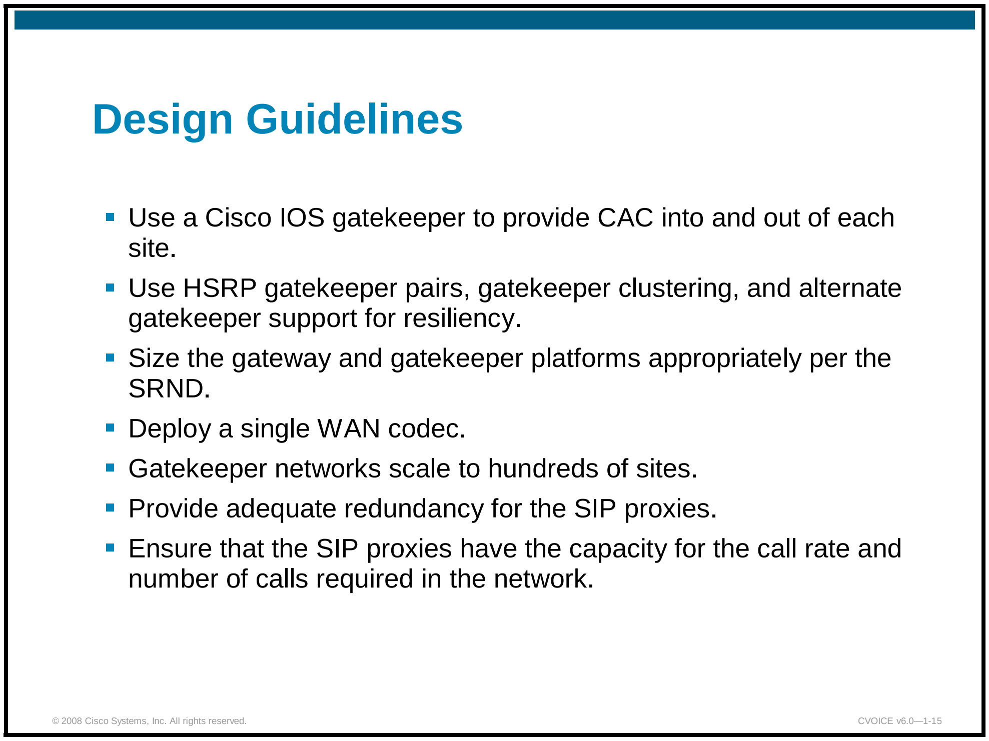
- Cost savings when you use the IP WAN for calls between sites
- Use of the IP WAN to bypass toll charges by routing calls through remote site gateways, closer to the PSTN number dialed

Note This practice is known as tail-end hop-off (TEHO).

- Maximum utilization of available bandwidth by allowing voice traffic to share the IP WAN with other types of traffic
- No loss of functionality during an IP WAN failure
- Scalability to hundreds of sites

Multisite Distributed Call Processing: Design Guidelines

The multisite WAN with distributed call-processing deployment model is a superset of the single-site and multisite WAN with centralized call-processing models.



Design Guidelines

- Use a Cisco IOS gatekeeper to provide CAC into and out of each site.
- Use HSRP gatekeeper pairs, gatekeeper clustering, and alternate gatekeeper support for resiliency.
- Size the gateway and gatekeeper platforms appropriately per the SRND.
- Deploy a single WAN codec.
- Gatekeeper networks scale to hundreds of sites.
- Provide adequate redundancy for the SIP proxies.
- Ensure that the SIP proxies have the capacity for the call rate and number of calls required in the network.

CVOICE v6.0—1-15

A multisite WAN deployment with distributed call processing has many of the same requirements as a single-site or a multisite WAN deployment with centralized call processing. Follow the best practices from these other models in addition to the ones listed here for the distributed call-processing model.

Gatekeeper or SIP proxy servers are among the key elements in the multisite WAN model with distributed call processing. They each provide dial plan resolution, with the gatekeeper also providing CAC. A gatekeeper is an H.323 device that provides CAC and E.164 dial plan resolution.

Best Practices

The following best practices apply to the use of a gatekeeper.

- Use a Cisco IOS gatekeeper to provide CAC into and out of each site.
- To provide high availability of the gatekeeper, use HSRP gatekeeper pairs, gatekeeper clustering, and alternate gatekeeper support. In addition, use multiple gatekeepers to provide redundancy within the network.
- Size the platforms appropriately to ensure that performance and capacity requirements can be met.
- Use only one type of codec on the WAN because the H.323 specification does not allow for Layer 2, IP, User Data Protocol (UDP), or RTP header overhead in the bandwidth request.

Note Header overhead is allowed only in the payload or encoded voice part of the packet.

Using one type of codec on the WAN simplifies capacity planning by eliminating the need to overprovision the IP WAN to allow for the worst-case scenario.

Gatekeeper networks can scale to hundreds of sites, and the design is limited only by the WAN topology.

SIP devices provide resolution of E.164 numbers as well as SIP Uniform Resource Identifiers (URIs) to enable endpoints to place calls to each other. Cisco Unified Communications Manager supports the use of E.164 numbers only.

The following best practices apply to the use of SIP proxies:

- Provide adequate redundancy for the SIP proxies.
- Ensure that the SIP proxies have the capacity for the call rate and number of calls that are required in the network.

Call-Processing Agents for the Distributed Call-Processing Model

Your choice of call-processing agent will vary, based on many factors. The main factors, for the purpose of design, are the size of the site and the required functionality.

For a distributed call-processing deployment, each site has its own call-processing agent. The design of each site varies with the call-processing agent, the required functionality, and the required fault tolerance. For example, in a site with 500 phones, a Cisco Unified Communications Manager cluster containing two servers can provide one-to-one redundancy, with the backup server being used as a publisher and Trivial File Transfer Protocol (TFTP) server.

The requirement for IP-based applications also greatly affects the choice of call-processing agent because only Cisco Unified Communications Manager provides the required support for many Cisco IP applications.

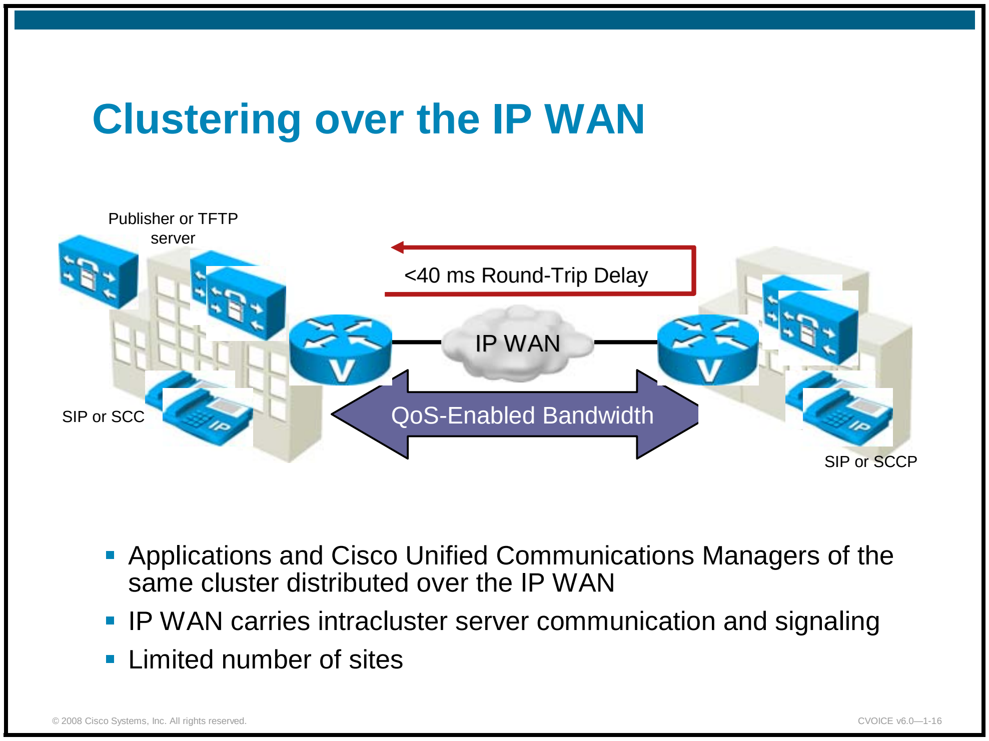
The table below lists recommended call-processing agents for distributed call processing.

Recommended Call-Processing Agents

Call-Processing Agent	Recommended Size	Comments
Cisco Unified Communications Manager Express	Up to 240 phones	■ For small remote sites ■ Capacity depends on Cisco IOS platform
Cisco Unified Communications Manager	50 to 30,000 phones	■ Small to large sites, depending on the size of the Cisco Unified Communications Manager cluster ■ Supports centralized or distributed call processing
Legacy PBX with VoIP gateway	Depends on PBX	■ Number of IP WAN calls and functionality depend on the PBX-to-VoIP gateway protocol and the gateway platform

Clustering over the IP WAN

This topic describes the characteristics, limitations, and advantages of clustering over the IP WAN.



Clustering over the IP WAN

- Applications and Cisco Unified Communications Managers of the same cluster distributed over the IP WAN
- IP WAN carries intracluster server communication and signaling
- Limited number of sites

CVOICE v6.0—1-16

Cisco supports Cisco Unified Communications Manager clusters over a WAN. In the clustering over WAN model, a single Cisco Unified Communications Manager cluster and its subscriber servers are split across multiple sites connected via a QoS-enabled WAN.

Clustering over the WAN can support two types of deployments:

- **Local failover deployment model:** Local failover requires that you place the Cisco Unified Communications Manager subscriber and backup servers at the same site, with no WAN between them. This deployment model is ideal for two to four sites with Cisco Unified Communications Manager.
- **Remote failover deployment model:** Remote failover allows you to deploy the backup servers over the WAN. Using this deployment model, you may have up to eight sites with Cisco Unified Communications Manager subscribers being backed up by Cisco Unified Communications Manager subscribers at another site.

Note The remote failover deployment model might need higher bandwidth because a large amount of intracluster traffic flows between the subscriber servers.

You can also use a combination of the two deployment models to satisfy specific site requirements. For example, two main sites may each have primary and backup subscribers, with another two sites containing only a primary server each and utilizing either shared backups or dedicated backups at the two main sites.

Benefits

Although there are stringent requirements, this design offers these advantages:

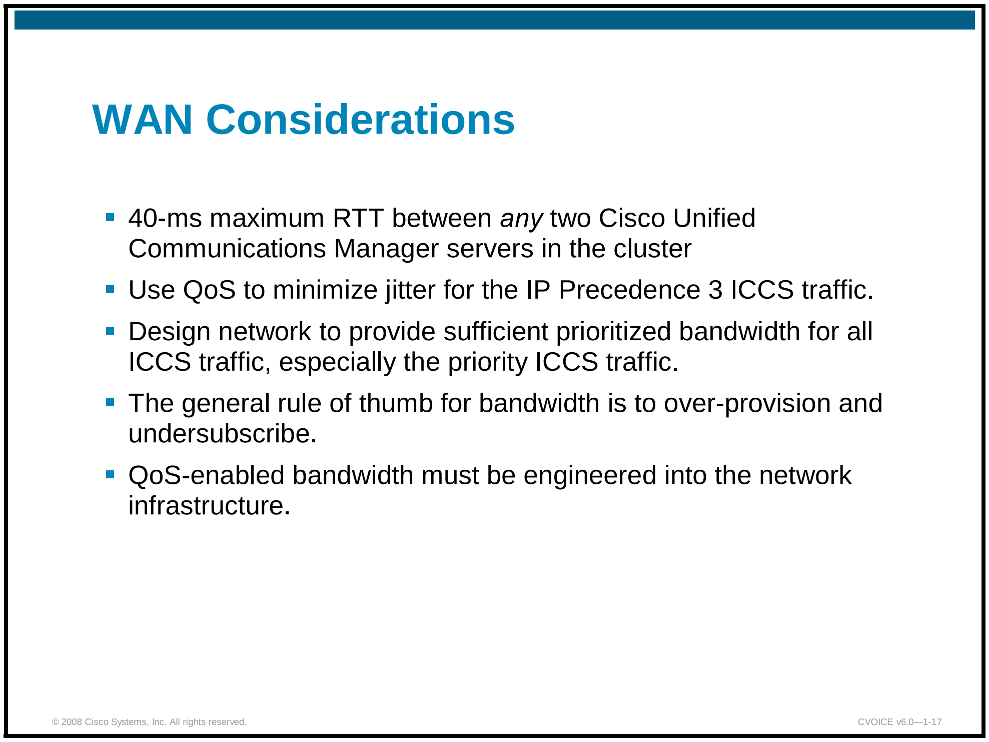
- Single point of administration for users for all sites within the cluster
- Feature transparency
- Shared line appearances
- Extension mobility within the cluster
- Unified dial plan

These features make this solution ideal as a disaster recovery plan for business continuance sites or as a single solution for up to eight small or medium sites.

The cluster design is also useful for customers who require more functionality than the limited feature set that is offered by SRST. This network design also allows remote offices to support more Cisco IP phones than SRST does in the event that the connection to the primary Cisco Unified Communications Manager is lost.

WAN Considerations

This subtopic covers some design guidelines for clustering over the WAN.



WAN Considerations

- 40-ms maximum RTT between *any* two Cisco Unified Communications Manager servers in the cluster
- Use QoS to minimize jitter for the IP Precedence 3 ICCS traffic.
- Design network to provide sufficient prioritized bandwidth for all ICCS traffic, especially the priority ICCS traffic.
- The general rule of thumb for bandwidth is to over-provision and undersubscribe.
- QoS-enabled bandwidth must be engineered into the network infrastructure.

CVOICE v6.0—1-17

For clustering over the WAN to be successful, you must carefully plan, design, and implement various characteristics of the WAN itself. The Intra-Cluster Communications Signaling (ICCS) between Cisco Unified Communications Manager servers consists of many traffic types. The ICCS traffic types are classified as either priority or best-effort. Priority ICCS traffic is marked with IP precedence 3. Best-effort ICCS traffic is marked with IP precedence 0.

The following design guidelines apply to the indicated WAN characteristics:

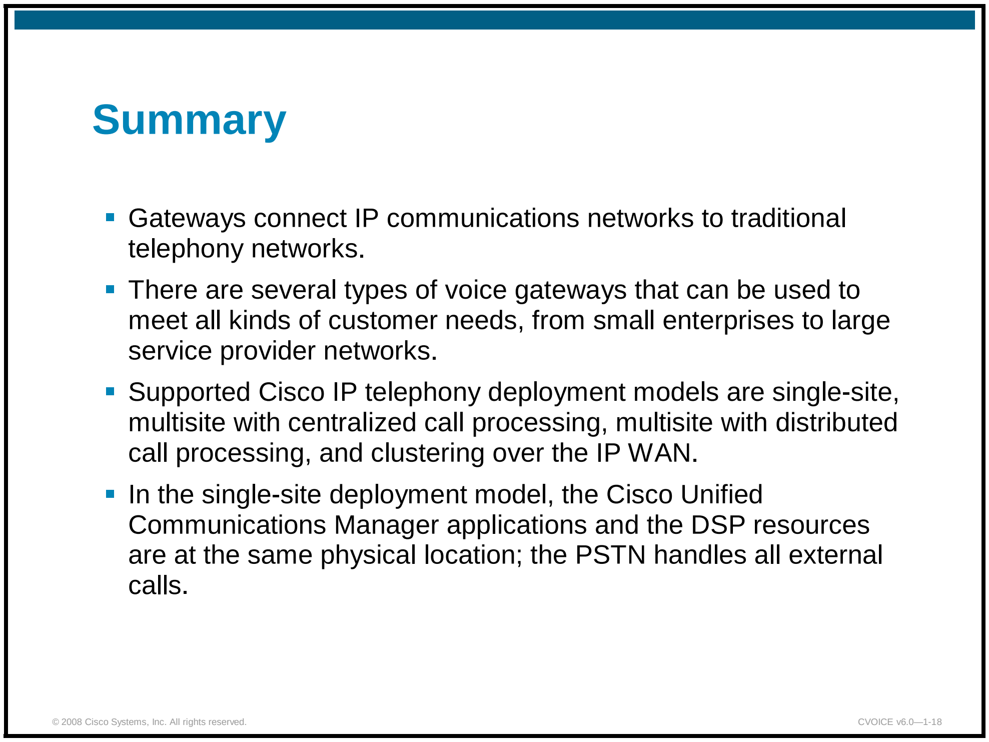
- **Delay:** The maximum one-way delay between any Cisco Unified Communications Manager servers for all priority ICCS traffic should not exceed 20 ms, or 40-ms round-trip time (RTT). Delay for other ICCS traffic should be kept reasonable to provide timely database access. Propagation delay between two sites introduces 6 microsec per kilometer without any other network delays being considered. This equates to a theoretical maximum distance of approximately 3000 km for 20-ms delay or approximately 1860 miles. These distances are provided only as relative guidelines and in reality will be shorter due to other delays incurred within the network.
- **Jitter:** Jitter is the varying delay that packets incur through the network due to processing, queue, buffer, congestion, or path variation delay. Jitter for the IP precedence 3 ICCS traffic must be minimized using QoS features.
- **Packet loss and errors:** The network should be engineered to provide sufficient prioritized bandwidth for all ICCS traffic, especially the priority ICCS traffic. Standard QoS mechanisms must be implemented to avoid congestion and packet loss. If packets are lost due to line errors or other “real world” conditions, the ICCS packet will be retransmitted because it uses TCP for reliable transmission. The retransmission might result in a call being delayed during setup or disconnect (teardown), or when other supplementary services are being performed during the call. Some packet loss conditions could result in a lost call,

but this scenario should be no more likely than errors occurring on a T1 or E1, which affect calls via a trunk to the PSTN or ISDN.

- **Bandwidth:** Provision the correct amount of bandwidth between each server for the expected call volume, type of devices, and number of devices. This bandwidth is in addition to any other bandwidth for other applications sharing the network, including voice and video traffic between the sites. The bandwidth provisioned must have QoS enabled to provide the prioritization and scheduling for the different classes of traffic. The general rule of thumb for bandwidth is to over-provision and under-subscribe.
- **Quality of Service:** The network infrastructure relies on QoS engineering to provide consistent and predictable end-to-end levels of service for traffic. Neither QoS nor bandwidth alone is the solution; rather, QoS-enabled bandwidth must be engineered into the network infrastructure.

Summary

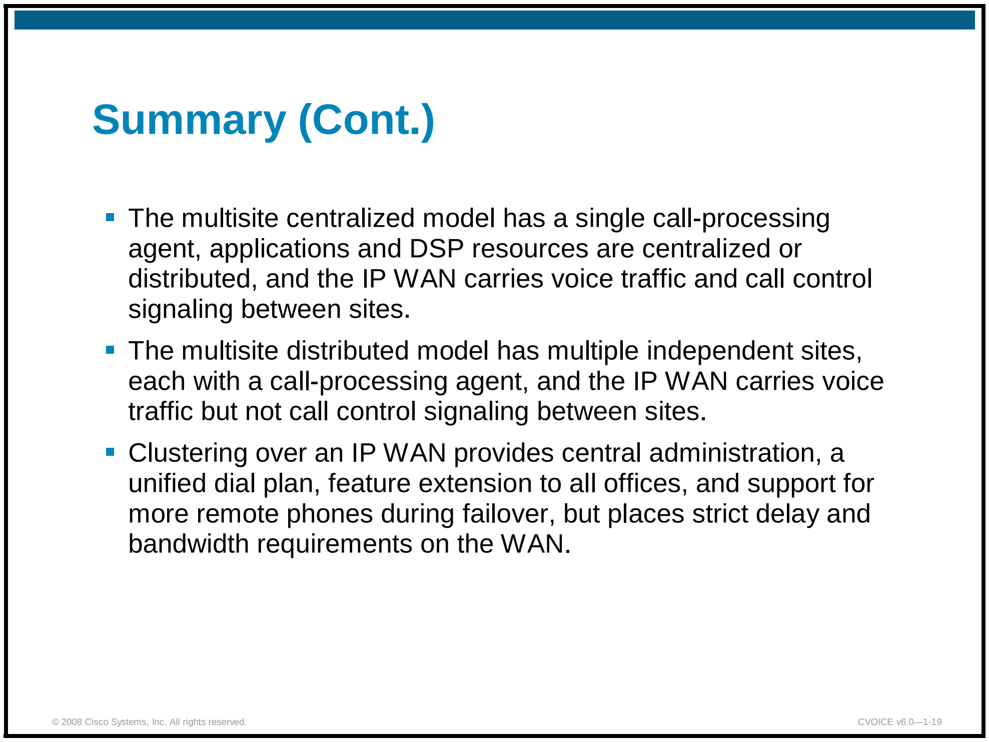
This topic summarizes the key points that were discussed in this lesson.



Summary

- Gateways connect IP communications networks to traditional telephony networks.
- There are several types of voice gateways that can be used to meet all kinds of customer needs, from small enterprises to large service provider networks.
- Supported Cisco IP telephony deployment models are single-site, multisite with centralized call processing, multisite with distributed call processing, and clustering over the IP WAN.
- In the single-site deployment model, the Cisco Unified Communications Manager applications and the DSP resources are at the same physical location; the PSTN handles all external calls.

CVOICE v6.0—1-18



Summary (Cont.)

- The multisite centralized model has a single call-processing agent, applications and DSP resources are centralized or distributed, and the IP WAN carries voice traffic and call control signaling between sites.
- The multisite distributed model has multiple independent sites, each with a call-processing agent, and the IP WAN carries voice traffic but not call control signaling between sites.
- Clustering over an IP WAN provides central administration, a unified dial plan, feature extension to all offices, and support for more remote phones during failover, but places strict delay and bandwidth requirements on the WAN.

CVOICE v6.0—1-19

Lesson Self-Check

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

Q1) IP communications _____ connect IP communications networks to traditional telephony networks.

Relates to: Understanding Gateways

Q2) Standalone gateways include the _____ and _____. (List two.)

Relates to: Gateway Hardware Platforms

Q3) The IP deployment models are the _____, _____, _____, and _____.

Relates to: IP Telephony Deployment Models

Q4) In the single-site deployment model, the Cisco Unified Communications Manager applications and the DSP resources are at the _____, and the _____ handles all external calls.

Relates to: Single-Site Deployment

Q5) In a multisite centralized model, the _____ carries voice traffic and call control signaling between sites.

Relates to: Multisite WAN with Centralized Call Processing

Q6) In a multisite distributed model, the IP WAN carries voice traffic between sites but not _____ signaling.

Relates to: Multisite WAN with Distributed Call Processing

Q7) Clustering over an IP WAN provides central administration places strict _____ and _____ requirements on the WAN

Relates to: Clustering over the IP WAN

Lesson Self-Check Answer Key

Q1) Gateways

Q2) VG224, VG248, AS5300, AS5400, ATA186

Q3) Single-site, multisite with centralized call processing, multisite with distributed call processing, clustering over the IP WAN

Q4) same physical location, PSTN

Q5) IP WAN

Q6) call control

Q7) delay, bandwidth

Lesson 3

Specifying Requirements for VoIP Calls

Overview

The inherent characteristics of a converged voice and data IP network cause network engineers and administrators to handle certain challenges in delivering voice traffic correctly. This lesson describes the challenges of integrating a voice and data network and offers solutions for avoiding problems when you are designing a VoIP network for optimal voice quality.

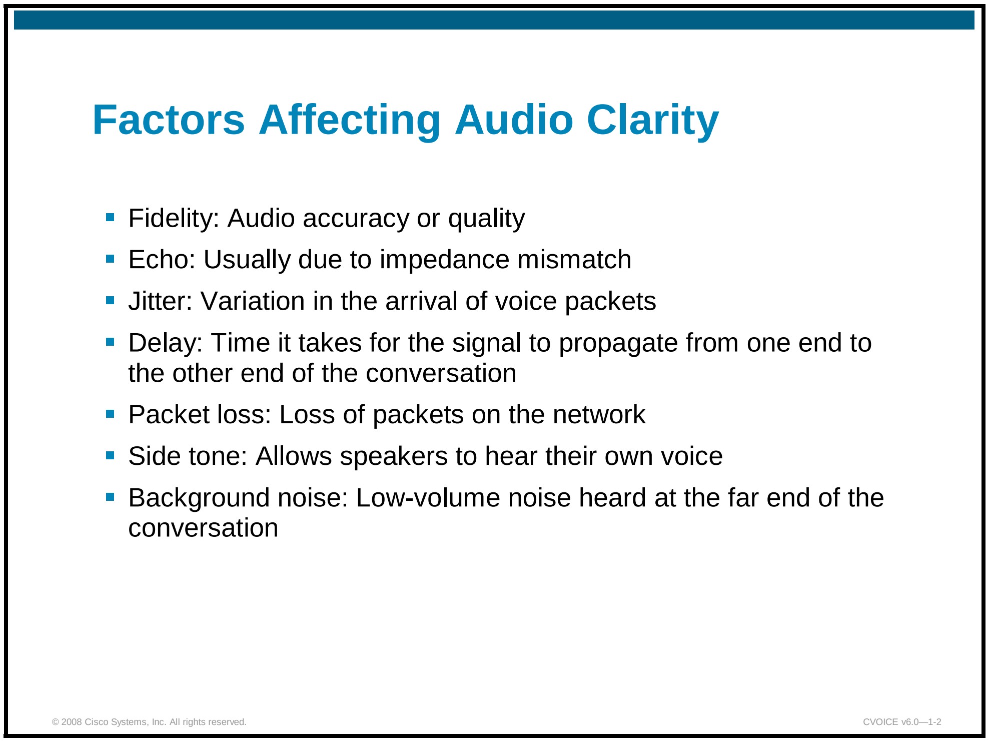
Objectives

Upon completing this lesson, you will be able to describe special requirements for VoIP calls including the need for quality of service (QoS) and fax relay, modem relay, and dual tone multifrequency (DTMF) support. This ability includes being able to meet these objectives:

- Describe the problems presented by IP networks in terms of audio clarity
- Describe MOS and PSQM and how they are used to measure audio quality
- Describe QoS features as they relate to a VoIP network and the features of Cisco IOS software that deliver QoS throughout the network
- Describe the challenge of transporting modulated data, including fax and modem calls, over IP networks
- Describe how fax and modem pass-through, relay, and store and forward are implemented using Cisco IOS gateways
- Describe how T.38 and pass-through are supported by H.323, SIP, and MGCP
- Describe DTMF relay and how it is supported in MGCP, H323, and SIP

IP Networking and Audio Clarity

This topic describes the factors in IP networks that affect audio clarity.



Factors Affecting Audio Clarity

- Fidelity: Audio accuracy or quality
- Echo: Usually due to impedance mismatch
- Jitter: Variation in the arrival of voice packets
- Delay: Time it takes for the signal to propagate from one end to the other end of the conversation
- Packet loss: Loss of packets on the network
- Side tone: Allows speakers to hear their own voice
- Background noise: Low-volume noise heard at the far end of the conversation

CVOICE v6.0—1-2

Because of the nature of IP networking, voice packets sent via IP are subject to certain transmission problems. Conditions that are present in the network may introduce problems such as echo, jitter, or delay. These problems must be addressed with QoS mechanisms.

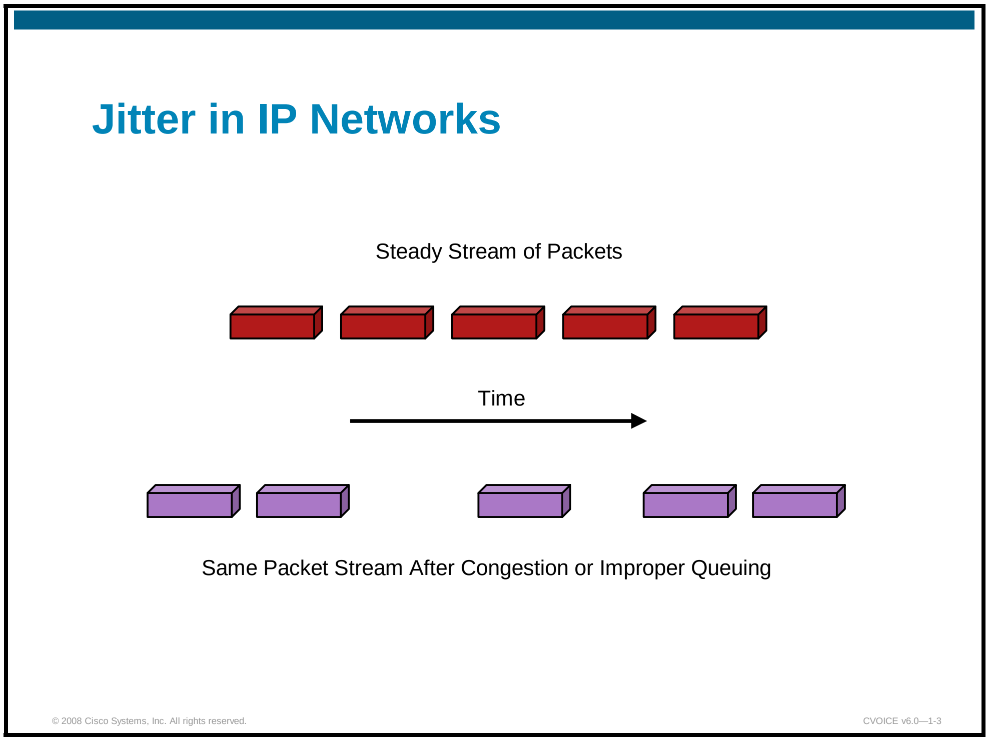
The clarity (or cleanliness and crispness) of the audio signal is of utmost importance. The listener must be able to recognize the identity and sense the mood of the speaker. These factors can affect clarity:

- **Fidelity:** Fidelity is the degree to which a system, or a portion of a system, accurately reproduces, at its output, the essential characteristics of the signal impressed upon its input or the result of a prescribed operation on the signal impressed upon its input (definition from the Alliance for Telecommunications Industry Solutions [ATIS]). The bandwidth of the transmission medium almost always limits the total bandwidth of the spoken voice. Human speech typically requires a bandwidth from 100 to 10,000 Hz, although 90 percent of speech intelligence is contained between 100 and 3000 Hz.
- **Echo:** Echo is a result of electrical impedance mismatches in the transmission path. Echo is always present, even in traditional telephony networks, but at a level that cannot be detected by the human ear. The two components that affect echo are amplitude (loudness of the echo) and delay (the time between the spoken voice and the echoed sound). You can control echo using suppressors or cancellers.
- **Jitter:** Jitter is variation in the arrival of coded speech packets at the far end of a VoIP network. The varying arrival time of the packets can cause gaps in the re-creation and playback of the voice signal. These gaps are undesirable and annoy the listener. Delay is induced in the network by variation in the routes of individual packets, contention, or congestion. You can resolve variable delay by using dejitter buffers.

- **Delay:** Delay is the time between the spoken voice and the arrival of the electronically delivered voice at the far end. Delay results from multiple factors, including distance (propagation delay), coding, compression, serialization, and buffers.
- **Packet loss:** Voice packets may be dropped under various conditions such as an unstable network, network congestion, or too much variable delay in the network. Lost voice packets are not recoverable, which results in gaps in the conversation that are perceptible to the user.
- **Side tone:** Side tone is the purposeful design of the telephone that allows the speaker to hear the spoken audio in the earpiece. Without side tone, the speaker is left with the impression that the telephone instrument is not working.
- **Background noise:** Background noise is the low-volume audio that is heard from the far-end connection. Certain bandwidth-saving technologies, such as voice activity detection (VAD), can eliminate background noise altogether. When VAD is implemented, the speaker audio path is open to the listener, while the listener audio path is closed to the speaker. The effect is often that speakers think that the connection is broken because they hear nothing from the other end.

Jitter

This subtopic describes the occurrence of jitter in IP networks and the Cisco solution to this problem.



Jitter in IP Networks

Steady Stream of Packets

Time

Same Packet Stream After Congestion or Improper Queuing

CVOICE v6.0—1-3

Jitter is defined as a variation in the arrival (delay) of received packets. On the sending side, packets are sent in a continuous stream, with the packets spaced evenly. Network congestion, improper queuing, or configuration errors can cause this steady stream to become uneven, because the delay between each packet varies instead of remaining constant, as displayed in the figure.

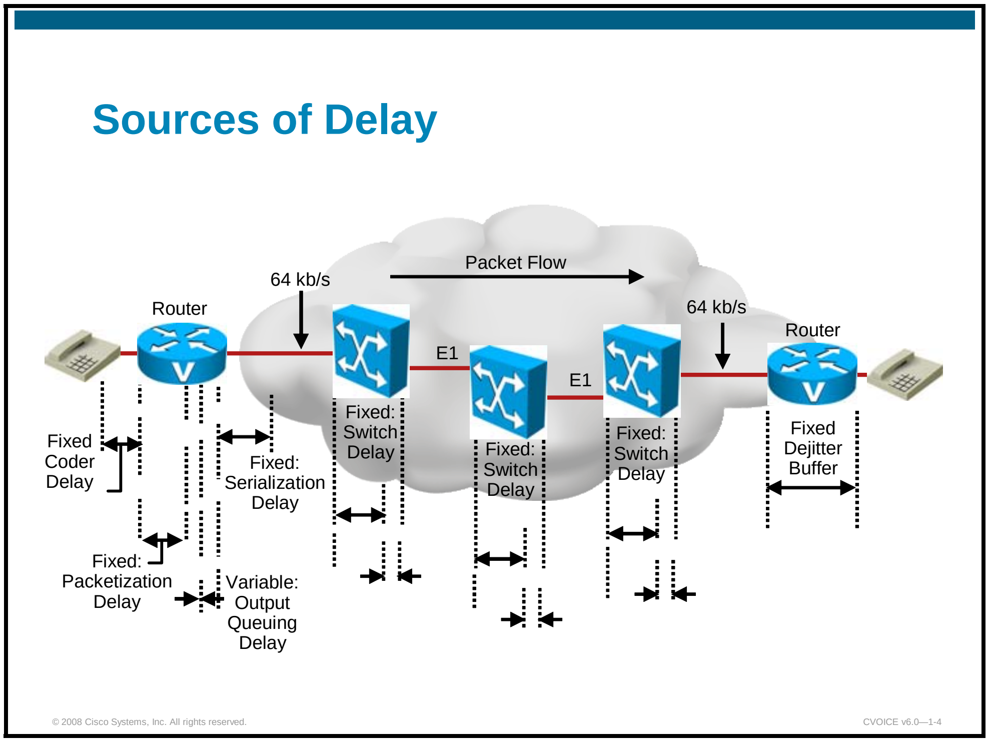
When a router receives an audio stream for VoIP, it must compensate for the jitter that is encountered. The mechanism that handles this function is the playout delay buffer, or dejitter buffer. The playout delay buffer must buffer these packets and then play them out in a steady stream to the digital signal processors (DSPs) to be converted back to an analog audio stream. The playout delay buffer, however, affects overall absolute delay.

Example

When a conversation is subjected to jitter, the results can be clearly heard. If the talker says, “Watson, come here. I want you,” the listener might hear, “Wat….s…on…….come here, I……wa……nt……..y……ou.” The variable arrival of the packets at the receiving end causes the speech to be delayed and garbled.

Delay

This subtopic describes the causes of packet delay and the Cisco solution to this problem.



Sources of Delay

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-4

Overall or absolute delay can affect VoIP. You may have experienced delay in a telephone conversation with someone on a different continent. The delays can cause entire words in the conversation to be cut off and can therefore be very frustrating.

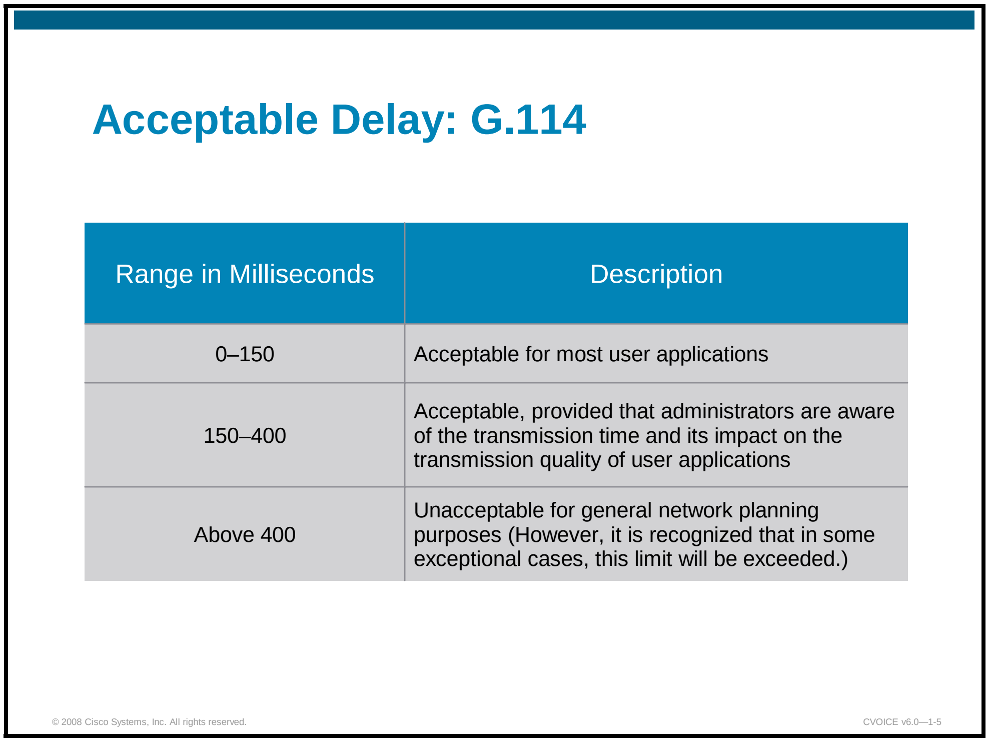
When you design a network that transports voice over packet, frame, or cell infrastructures, it is important to understand and account for the predictable delay components in the network. You must also correctly account for all potential delays to ensure that overall network performance is acceptable. Overall voice quality is a function of many factors, including the compression algorithm, errors and frame loss, echo cancellation, and delay.

Here are the two distinct types of delay:

- **Fixed delay:** Fixed-delay components are predictable and add directly to overall delay on the connection. Fixed-delay components include those listed here:
  - **Coding:** The time that it takes to translate the audio signal into a digital signal
  - **Packetization:** The time that it takes to put digital voice information into packets and remove the information from packets
  - **Serialization:** The insertion of bits onto a link
  - **Propagation:** The time that it takes a packet to traverse a link
- **Variable delays:** Variable delays arise from queuing delays in the egress trunk buffers that are located on the serial port that is connected to the WAN. These buffers create variable delays, called jitter, across the network.

Acceptable Delay

This subtopic describes the level of delay defined as acceptable by the G.114 standard.



Acceptable Delay: G.114

Range in Milliseconds	Description
0–150	Acceptable for most user applications
150–400	Acceptable, provided that administrators are aware of the transmission time and its impact on the transmission quality of user applications
Above 400	Unacceptable for general network planning purposes (However, it is recognized that in some exceptional cases, this limit will be exceeded.)

CVOICE v6.0—1-5

ITU-T specifies network delay for voice applications in ITU-T Recommendation G.114. This recommendation defines three bands of one-way delay, as shown in the table in the figure.

Note This recommendation is for connections with echo that are adequately controlled, implying that echo cancellers are used. Echo cancellers are required when one-way delay exceeds 25 ms (ITU-T Recommendation G.131).

This recommendation is designed for national telecommunications administrations and, therefore, is more stringent than recommendations that would normally be applied in private voice networks. When the location and business needs of end users are well known to a network designer, more delay may prove acceptable. For private networks, a 200-ms delay is a reasonable goal and a 250-ms delay is the limit. This goal is what Cisco proposes as reasonable as long as excessive jitter does not affect voice quality. However, all networks must be engineered so that the maximum expected voice connection delay is known and minimized.

Calculating Delay Budget

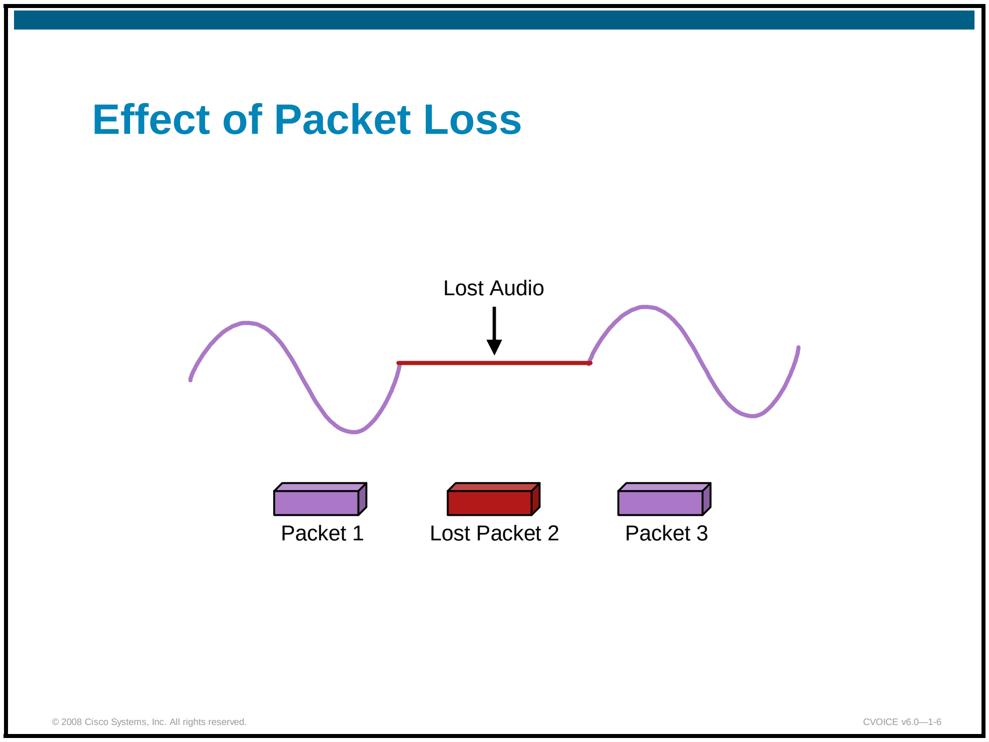
The G.114 recommendation is for one-way delay only and does not account for round-trip delay. Network design engineers must consider both variable and fixed delays. Variable delays include queuing and network delays, while fixed delays include coding, packetization, serialization, and dejitter buffer delays. The “Delay Budget Calculations” table is an example of calculating delay budget.

Delay Budget Calculations

Delay Type	Fixed (ms)	Variable (ms)
Coder delay	18	—
Packetization delay	30	—
Queuing and buffering	—	8
Serialization (64 kb/s)	5	—
Network delay (public frame)	40	25
Dejitter buffer	45	—
Totals	138	33

Packet Loss

This subtopic describes the causes and effects of lost voice packets.



Effect of Packet Loss

CVOICE v6.0—1-6

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.

Voice packets may be dropped under these conditions:

- The network is unstable (flapping links).
- The network is congested.
- There is too much variable delay in the network.

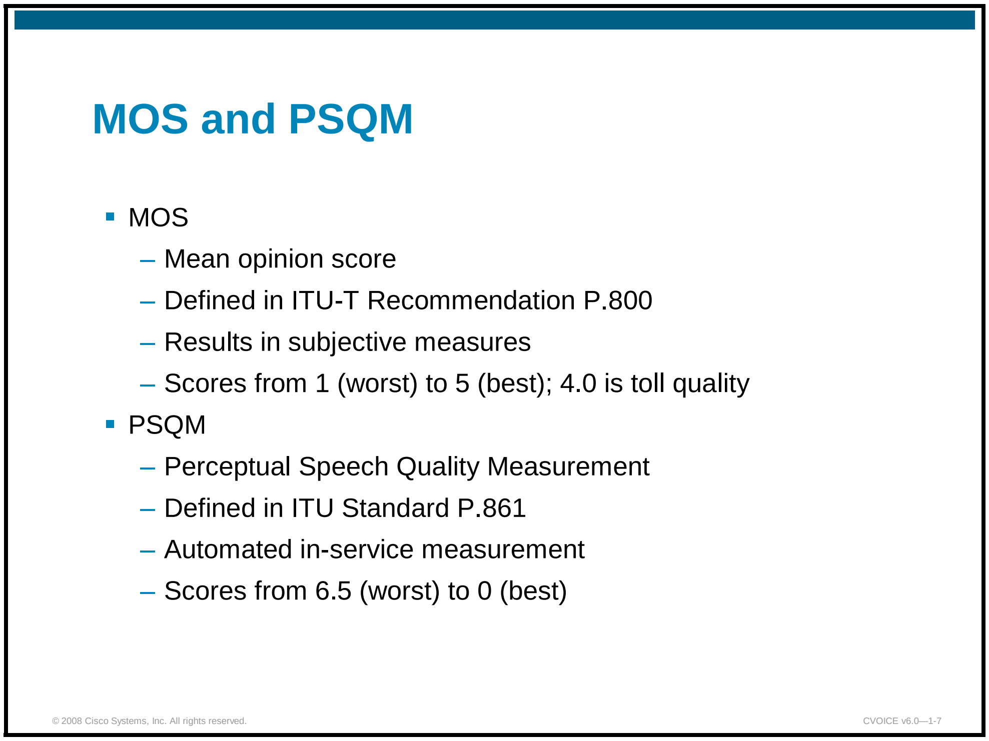
Packet loss causes voice clipping and skips. As a result, the listener hears gaps in the conversation, as shown in the figure. The industry standard coder-decoder (codec) algorithms that are used in Cisco DSPs will correct for 20 to 50 ms of lost voice through the use of Packet Loss Concealment (PLC) algorithms. PLC intelligently analyzes missing packets and generates a reasonable replacement packet to improve the voice quality. Cisco VoIP technology uses 20-ms samples of voice payload per VoIP packet by default. Effective codec correction algorithms require that only a single packet can be lost at any given time. If more packets are lost, the listener experiences gaps.

Example

If a conversation experiences packet loss, the effect is immediately heard. If the talker says, “Watson, come here. I want you,” the listener might hear, “Wat----, come here, ------you.”

Audio Quality Measurement

This topic describes mean opinion score (MOS) and Perceptual Speech Quality Measurement (PSQM) and how they are used to measure audio quality in VoIP networks.



MOS and PSQM

- MOS
  - Mean opinion score
  - Defined in ITU-T Recommendation P.800
  - Results in subjective measures
  - Scores from 1 (worst) to 5 (best); 4.0 is toll quality
- PSQM
  - Perceptual Speech Quality Measurement
  - Defined in ITU Standard P.861
  - Automated in-service measurement
  - Scores from 6.5 (worst) to 0 (best)

CVOICE v6.0—1-7

Mean Opinion Score

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. The sentence used for English-language MOS testing is, “Nowadays, a chicken leg is a rare dish.” This sentence is used because it contains a wide range of sounds found in human speech, such as long vowels, short vowels, hard sounds, and soft sounds.

The test scores are then averaged to a composite score. The test results are subjective because they are based on the opinions of the listeners. The tests are also relative because a score of 3.8 from one test cannot be directly compared to a score of 3.8 from another test. Therefore, you must establish a baseline for all tests, such as G.711, so that the scores can be normalized and compared directly.

Perceptual Speech Quality Measurement

PSQM is an automated method of measuring speech quality “in service,” or as the speech happens. PSQM software usually resides with IP call management systems, which are sometimes integrated into Simple Network Management Protocol (SNMP) systems.

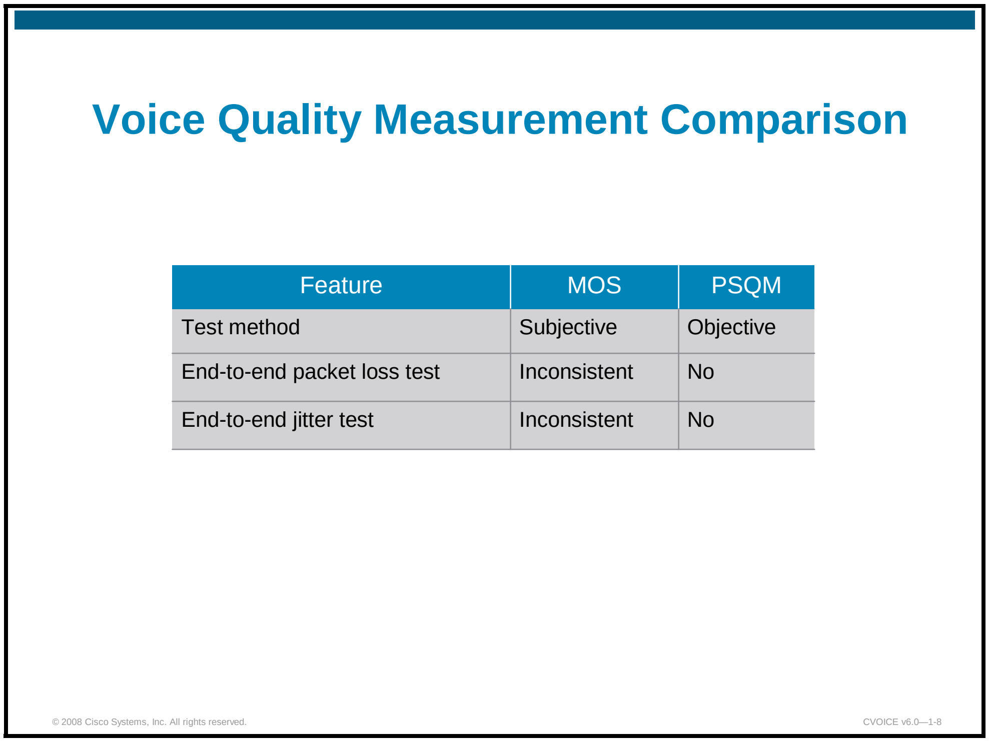
Equipment and software that can measure PSQM are available through third-party vendors; they are not implemented in Cisco equipment. The measurement is made by comparing the original transmitted speech to the resulting speech at the far end of the transmission channel. PSQM systems are deployed as in-service components. The PSQM measurements are made during real conversation on the network. This automated testing algorithm has over 90 percent accuracy compared to subjective listening tests, such as MOS. Scoring is based on a scale from 0 to 6.5, where 0 is the best and 6.5 is the worst. Because it was originally designed for circuit-switched voice, PSQM does not take into account the jitter or delay problems that are experienced in packet-switched voice systems.

MOS and PSQM in VoIP Networks

MOS and PSQM are not recommended for present-day VoIP networks. Both were originally designed before the emergence of VoIP technologies and do not measure typical VoIP problems such as jitter and delay. For example, it is possible to obtain an MOS score of 3.8 on a VoIP network when the one-way delay exceeds 500 ms because the MOS evaluator has no concept of a two-way conversation and listens only to audio quality. The one-way delay is not evaluated.

Quality Measurement Comparison

Early quality measurement methods, such as MOS and PSQM, were designed before widespread acceptance of VoIP technology. Perceptual Evaluation of Speech Quality (PESQ) was designed to address the shortcomings of MOS and PSQM.



Voice Quality Measurement Comparison

Feature	MOS	PSQM
Test method	Subjective	Objective
End-to-end packet loss test	Inconsistent	No
End-to-end jitter test	Inconsistent	No

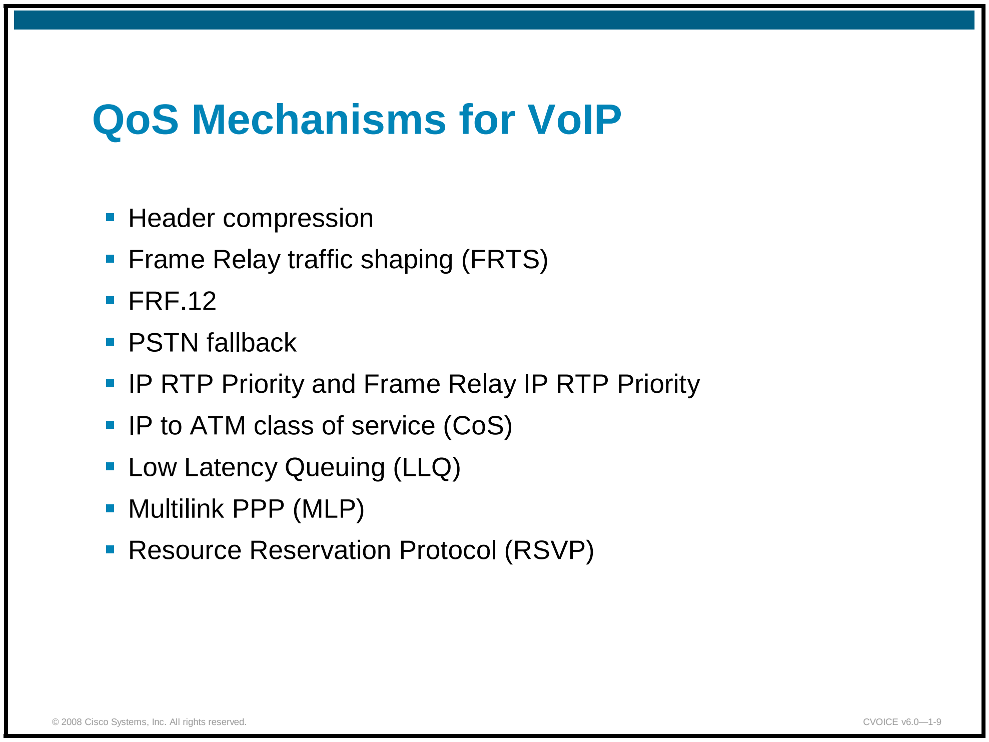
CVOICE v6.0—1-8

MOS uses subjective testing in which the average opinion of a group of test users is calculated to create the MOS score. This method is both time-consuming and expensive and may not provide consistent results between groups of testers.

PSQM uses objective testing in which an original reference file sent into the system is compared with the impaired signal that came out. This testing method provides an automated test mechanism that does not rely on human interpretation for result calculations. However, PSQM was originally designed for circuit-switched networks and does not take into account the effects of jitter and packet loss.

VoIP and QoS

This topic describes QoS issues as they relate to a VoIP network.



QoS Mechanisms for VoIP

- Header compression
- Frame Relay traffic shaping (FRTS)
- FRF.12
- PSTN fallback
- IP RTP Priority and Frame Relay IP RTP Priority
- IP to ATM class of service (CoS)
- Low Latency Queuing (LLQ)
- Multilink PPP (MLP)
- Resource Reservation Protocol (RSVP)

CVOICE v6.0—1-9

Real-time applications such as voice applications have different characteristics and requirements from those of traditional data applications. Because they are real-time-based, voice applications tolerate minimal variation in the amount of delay that affects delivery of their voice packets. Voice traffic is also intolerant of packet loss and jitter, both of which unacceptably degrade the quality of the voice transmission delivered to the recipient end user. To effectively transport voice traffic over IP, mechanisms that ensure reliable delivery of voice packets are required. Cisco IOS QoS features collectively embody these techniques, offering the means to provide priority service that meets the stringent requirements of voice packet delivery.

The QoS components for Cisco Unified Communications are provided through the rich IP traffic management, queuing, and shaping capabilities of the Cisco IP network infrastructure.

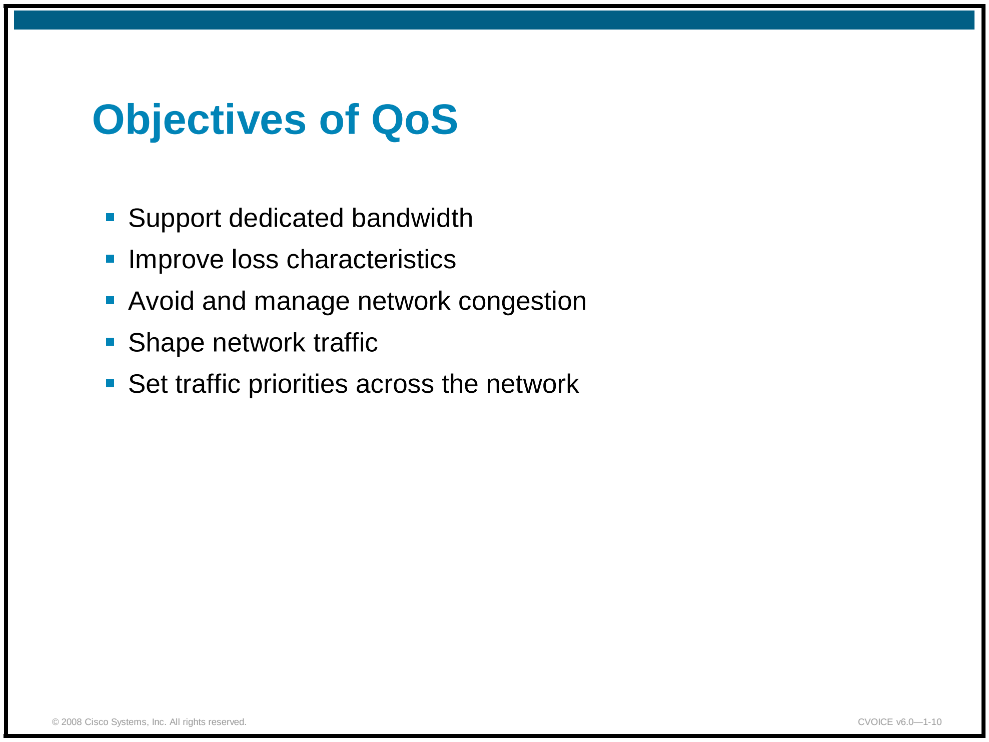
Following are a few of the Cisco IOS features that address the requirements of end-to-end QoS and service differentiation for voice packet delivery:

- **Header compression:** Used in conjunction with Real-Time Transport Protocol (RTP) and TCP, compresses the extensive RTP or TCP header, resulting in decreased consumption of available bandwidth for voice traffic. A corresponding reduction in delay is realized.
- **Frame Relay traffic shaping (FRTS):** Delays excess traffic using a buffer, or queuing mechanism, to hold packets and shape the flow when the data rate of the source is higher than expected.
- **Frame Relay Fragmentation Implementation Agreement (FRF.12) (and higher):** Ensures predictability for voice traffic, aiming to provide better throughput on low-speed Frame Relay links by interleaving delay-sensitive voice traffic on one virtual circuit (VC) with fragments of a long frame on another VC utilizing the same interface.

- **Public switched telephone network (PSTN) fallback:** Provides a mechanism to monitor congestion in the IP network and either redirect calls to the PSTN or reject calls based on the network congestion.
- **IP RTP Priority and Frame Relay IP RTP Priority:** Provides a strict priority queuing scheme that allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued. These features are especially useful on slow-speed WAN links, including Frame Relay, MLP, and T1 ATM links. It works with weighted fair queuing (WFQ) and class-based WFQ (CBWFQ).
- **IP-to-ATM class of service (CoS):** Includes a feature suite that maps QoS characteristics between IP and ATM. Offers differential service classes across the entire WAN, not just the routed portion. Gives mission-critical applications exceptional service during periods of high network usage and congestion.
- **Low Latency Queuing (LLQ):** Provides strict priority queuing on ATM VCs and serial interfaces. This feature allows you to configure the priority status for a class within CBWFQ and is not limited to User Datagram Protocol (UDP) port numbers, as is IP RTP Priority.
- **Multilink PPP (MLP):** Allows large packets to be multilink-encapsulated and fragmented so that they are small enough to satisfy the delay requirements of real-time traffic. MLP also provides a special transmit queue for the smaller, delay-sensitive packets, enabling them to be sent earlier than other flows.
- **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 supporting VoIP, RSVP—in conjunction with features that provide queuing, traffic shaping, and voice call signaling—can provide Call Admission Control (CAC) for voice traffic. Cisco also provides RSVP support for LLQ and Frame Relay.

Objectives of QoS

This subtopic discusses how QoS can help improve voice quality in a VoIP environment.



Objectives of QoS

- Support dedicated bandwidth
- Improve loss characteristics
- Avoid and manage network congestion
- Shape network traffic
- Set traffic priorities across the network

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-10

To ensure that VoIP is an acceptable replacement for standard PSTN telephony services, customers must receive the same consistently high quality of voice transmission that they receive with basic telephone services.

Like other real-time applications, VoIP is extremely sensitive to issues related to bandwidth and delay. To ensure that VoIP transmissions are intelligible to the receiver, voice packets cannot be dropped, excessively delayed, or subject to variations in delay (jitter). A successful VoIP deployment must provide an acceptable level of voice quality by meeting VoIP traffic requirements for issues related to bandwidth, latency, and jitter.

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Frame Relay, ATM, Ethernet and IEEE 802.1 networks, SONET, and IP-routed networks. VoIP guarantees high-quality voice transmission only if the signaling and audio channel packets have priority over other kinds of network traffic.

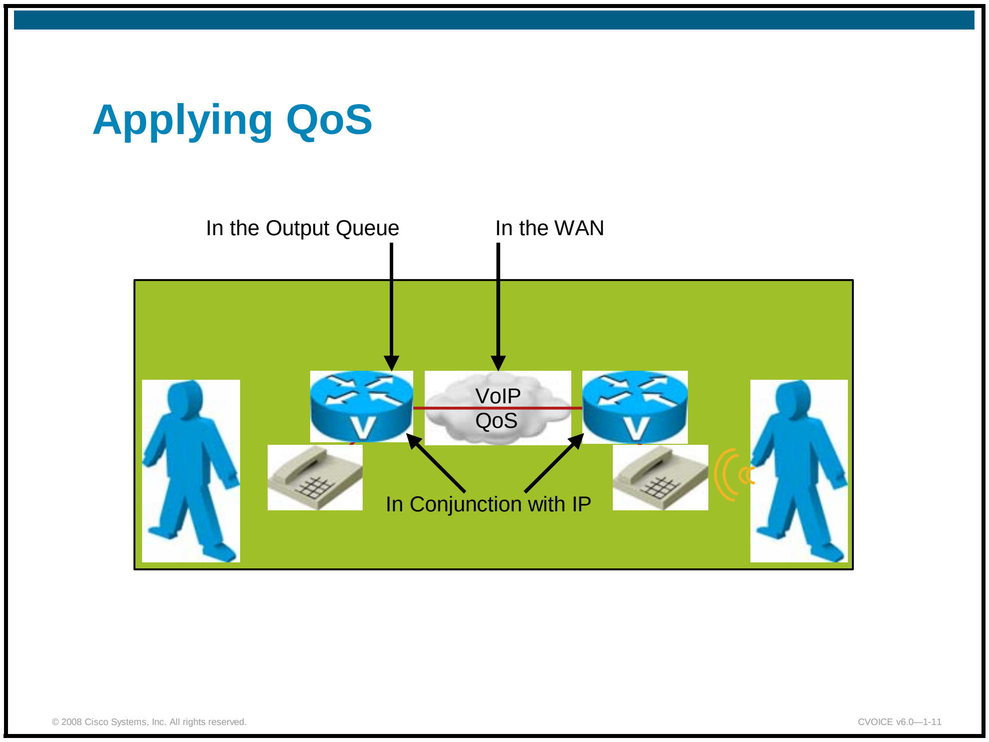
In particular, QoS features provide improved and more predictable network operations by implementing these objectives:

- **Support guaranteed bandwidth:** Designing the network such that the necessary bandwidth is always available to support voice and data traffic
- **Improve loss characteristics:** Designing the Frame Relay network such that discard eligibility is not a factor for frames containing voice, keeping voice below the committed information rate (CIR)
- **Avoid and manage network congestion:** Ensuring that the LAN and WAN infrastructure can support the volume of data traffic and voice calls

- **Shape network traffic:** Using Cisco traffic-shaping tools to ensure smooth and consistent delivery of frames to the WAN
- **Set traffic priorities across the network:** Marking the voice traffic as priority and queuing it first

Using QoS to Improve Voice Quality

This subtopic identifies the network areas in which QoS is implemented in Cisco networks.



Applying QoS

In the Output Queue

In the WAN

VoIP
QoS

In Conjunction with IP

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—1-11

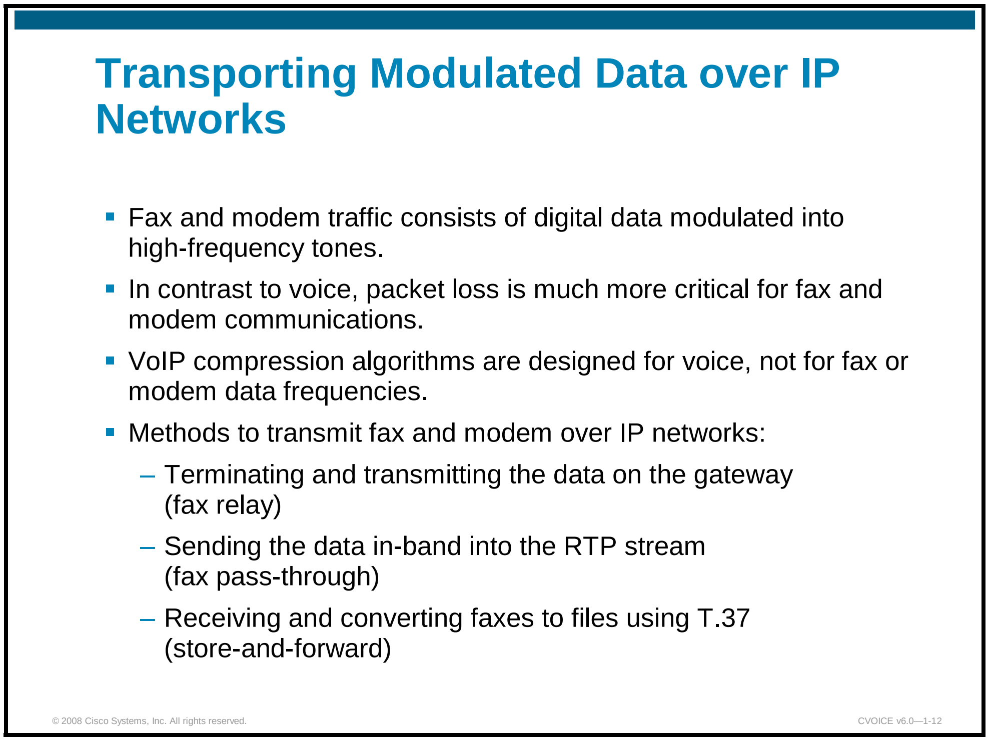
Voice features that provide QoS are deployed at different points in the network and designed for use with other QoS features to achieve specific goals, such as minimization of jitter and delay.

Cisco IOS software includes a complete set of features for delivering QoS throughout the network. Output queuing, such as LLQ, is one of the Cisco IOS features that address the voice packet delivery requirements of end-to-end QoS and service differentiation. LLQ provides strict priority queuing (PQ) in conjunction with CBWFQ. LLQ configures the priority status for a class within CBWFQ in which voice packets receive priority over all other traffic. LLQ is considered a best practice by the Cisco Enterprise Solutions Engineering (ESE) group for delivering voice QoS services over a WAN.

Note	Other individual queuing mechanisms are covered in the *Quality of Service* course.

Transporting Modulated Data over IP Networks

This topic describes the challenge of transporting modulated data, including fax and modem calls, over IP networks.



Transporting Modulated Data over IP Networks

- Fax and modem traffic consists of digital data modulated into high-frequency tones.
- In contrast to voice, packet loss is much more critical for fax and modem communications.
- VoIP compression algorithms are designed for voice, not for fax or modem data frequencies.
- Methods to transmit fax and modem over IP networks:
  - Terminating and transmitting the data on the gateway (fax relay)
  - Sending the data in-band into the RTP stream (fax pass-through)
  - Receiving and converting faxes to files using T.37 (store-and-forward)

CVOICE v6.0—1-12

An IP, or packet-switched, network enables data to be sent in packets to remote locations. The data is assembled by a packet assembler/disassembler (PAD) into individual packets of data, involving a process of segmentation or subdivision of larger sets of data as specified by the native protocol of the sending device. Each packet has a unique identifier that makes it independent and has its own destination address. Because the packet is unique and independent, it can traverse the network in a stream of packets and use different routes. This fact has some implications for fax transmissions that use data packets instead of an analog signal over a circuit-switched network.

Differences from Fax Transmission in the PSTN

In IP networks, individual packets that are part of the same data transmission may follow different physical paths of varying lengths. They can also experience varying levels of propagation delay (latency) and delay that is caused by packets being held in packet buffers awaiting the availability of a subsequent circuit. The packets can also arrive in an order different from the order in which they entered the network. The destination node of the network uses the identifiers and addresses in the packet sequencing information to reassemble the packets into the correct sequence.

Fax transmissions are designed to operate across a 64-kb/s pulse code modulation (PCM)-encoded voice circuit, but in packet networks, the 64-kb/s stream is often compressed into a much smaller data rate by passing it through a DSP. The codecs normally used to compress a voice stream in a DSP are designed to compress and decompress human speech, not fax or modem tones. For this reason, faxes and modems are rarely used in a VoIP network without some kind of relay or pass-through mechanism in place.

Fax Services over IP Networks

There are three conceptual methods of carrying virtual real-time fax machine–to–fax machine communications across packet networks:

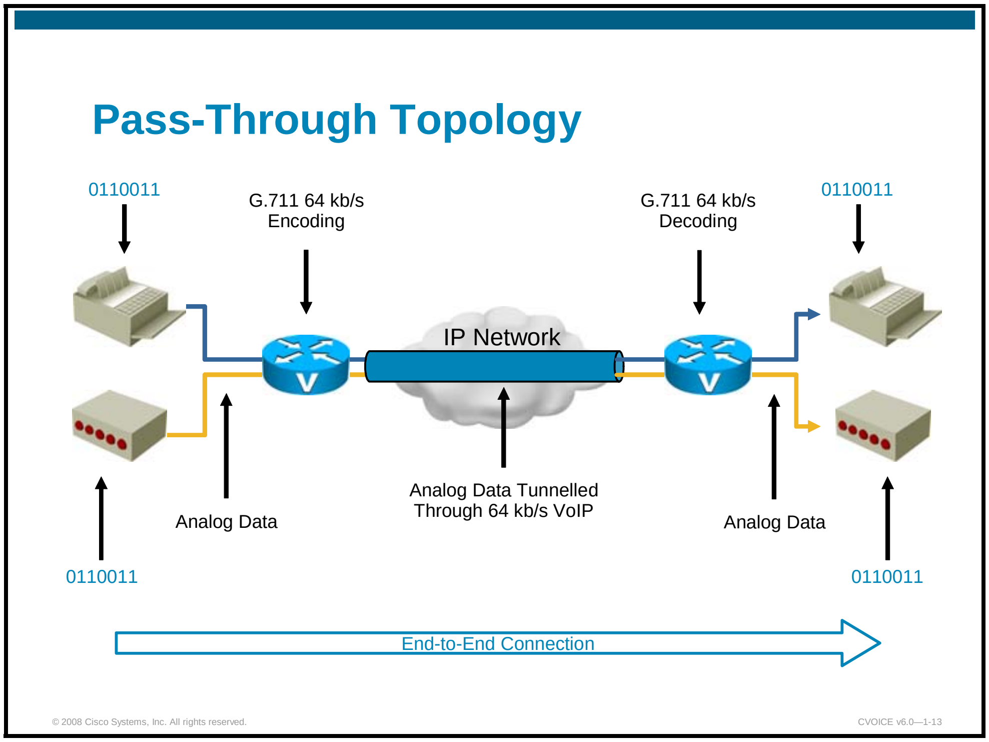
- **Fax relay:** The T.30 fax from the PSTN is demodulated at the sending gateway. The demodulated fax content is enveloped into packets, sent over the network, and remodulated into T.30 fax at the receiving end.

Note Cisco IOS software supports T.38 and Cisco fax relay (proprietary).

- **Fax pass-through:** Modulated fax information from the PSTN is passed in-band end-to-end over a voice speech path in an IP network. There are two pass-through techniques:
  - The configured voice codec is used for the fax transmission. This technique works only when the configured codec is G.711 with no VAD and no echo cancellation, or when the configured codec is a clear-channel (G.Clear) codec or G.726 or G.732. Low bit-rate codecs cannot be used for fax transmissions.
  - The gateway dynamically changes the codec from the codec configured for voice to G.711 with no VAD and no echo cancellation for the duration of the fax session. This method is specifically referred to as codec "upspeed" or fax pass-through with upspeed.
- **Store-and-forward fax:** Breaks the fax process into distinct sending and receiving processes and allows fax messages to be stored between those processes. Store-and-forward fax is based on the ITU-T T.37 standard, and it also enables fax transmissions to be received from or delivered to computers rather than fax machines.

Understanding Fax and Modem Pass-Through, Relay, and Store and Forward

This topic describes how fax and modem pass-through, relay, and store and forward are implemented using Cisco IOS gateways.



Pass-Through Topology

0110011

G.711 64 kb/s
Encoding

G.711 64 kb/s
Decoding

0110011

IP Network

Analog Data

Analog Data Tunnelled
Through 64 kb/s VoIP

Analog Data

0110011

0110011

End-to-End Connection

CVOICE v6.0—1-13

Several features are available to overcome the issues that are involved with carrying fax and modem signals across an IP network:

- Fax and modem pass-through
- Fax and modem relay
- Fax store and forward

Fax Pass-Through

With fax pass-through, modulated fax information from the PSTN is passed in-band over a voice speech path in an IP network.

Fax pass-through is the simplest technique for sending fax over IP networks, but it is not the default, nor is it the most desirable method of supporting fax over IP. T.38 fax relay provides a more reliable and error-free method of sending faxes over an IP network, but some third-party H.323 and session initiation protocol (SIP) implementations do not support T.38 fax relay. These same implementations often support fax pass-through.

Fax pass-through is also known as voice band data by the ITU. Voice band data refers to the transport of fax or modem signals over a voice channel through a packet network with an encoding appropriate for fax or modem signals. The minimum set of coders for voice band data mode is G.711 mu-law and a-law with VAD disabled.

Fax pass-through takes place when incoming T.30 fax data is not demodulated or compressed for its transit through the packet network. The two endpoints (fax machines or modems) communicate directly to each other over a transparent IP connection. The gateway does not distinguish fax calls from voice calls.

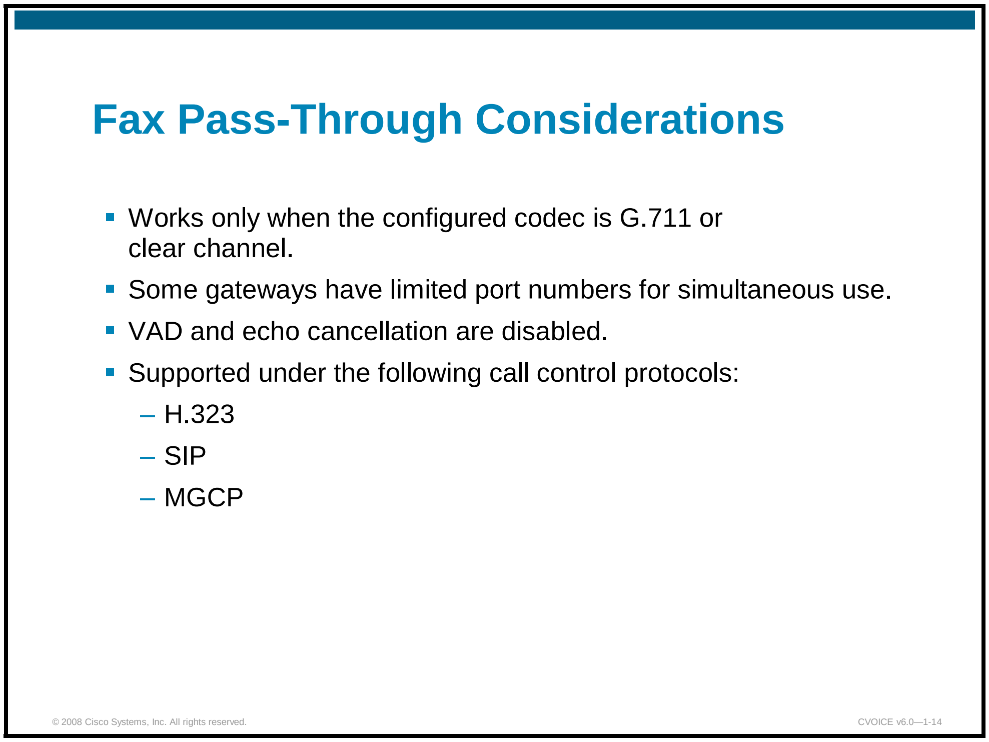
On detection of a fax tone on an established VoIP call, the gateways switch into fax pass-through mode by suspending the voice codec and loading the pass-through parameters for the duration of the fax session. This process, called upspeeding, changes the bandwidth that is needed for the call to the equivalent of G.711.

With pass-through, the fax traffic is carried between the two gateways in RTP packets using an uncompressed format resembling the G.711 codec. This method of transporting fax traffic takes a constant 64-kb/s (payload) stream plus its IP overhead end to end for the duration of the call. IP overhead is 16 kb/s for normal voice traffic, but when using fax pass-through, the packetization period is reduced from 20 ms to 10 ms, which means that half as much data can be put into each frame. The result is that you need twice as many frames and twice as much IP overhead. For pass-through, the total bandwidth is 64 plus 32 kb/s, for a total of 96 kb/s. For normal voice traffic, total bandwidth is 64 plus 16 kb/s, for a total of 80 kb/s. The table compares a G.711 VoIP call that uses 20-ms packetization with a G.711 fax pass-through call that uses 10-ms packetization.

Packetization	G.711 Payload	Overhead for Layers 3 and 4	Packet Size	Bit Rate
10 ms	80 byte	40 byte	120 byte	96 kb/s
20 ms	160 byte	40 byte	200 byte	80 kb/s

Packet redundancy may be used to mitigate the effects of packet loss in the IP network. Even so, fax pass-through remains susceptible to packet loss, jitter, and latency in the IP network. The two endpoints must be clocked synchronously for this type of transport to work predictably.

Performance may become an issue. To attempt to mitigate packet loss in the network, redundant encoding (1*x* or one repeat of the original packet) is used, which doubles the amount of data transferred in each packet. The doubling of packets imposes a limitation on the total number of ports that can run fax pass-through at one time. One fax pass-through session with redundancy needs as much bandwidth as two G.711 calls without VAD.



Fax Pass-Through Considerations

- Works only when the configured codec is G.711 or clear channel.
- Some gateways have limited port numbers for simultaneous use.
- VAD and echo cancellation are disabled.
- Supported under the following call control protocols:
  - H.323
  - SIP
  - MGCP

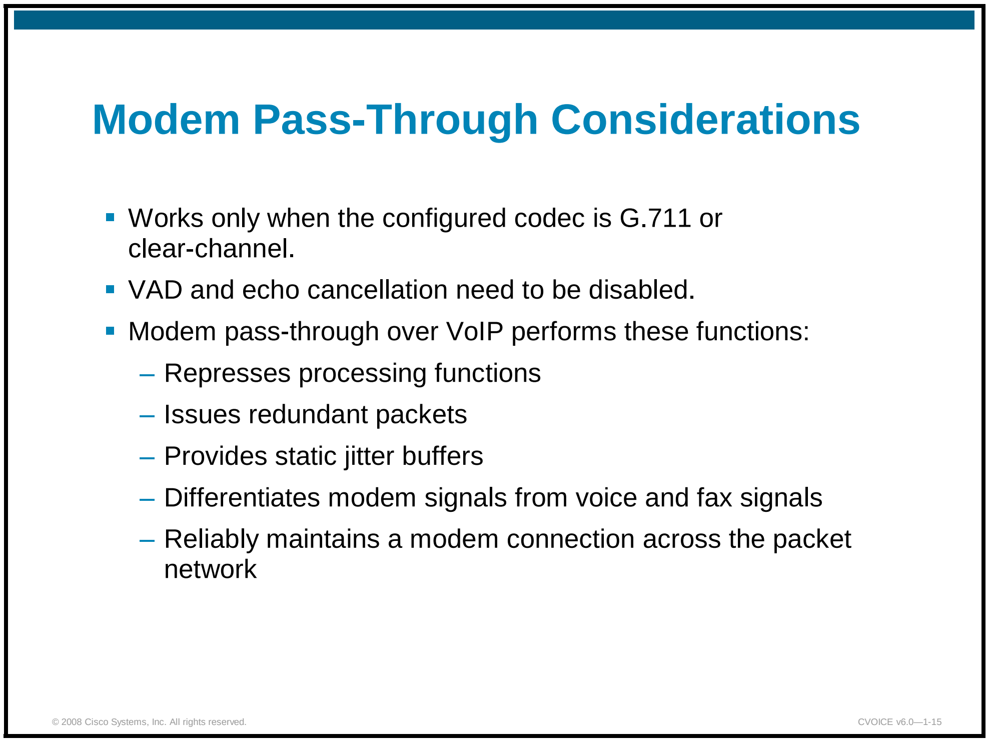
CVOICE v6.0—1-14

Consider these factors when determining whether to use fax pass-through.

- Fax pass-through does not support the switch from G.Clear to G.711. If fax pass-through and the G.Clear codec are both configured, the gateway cannot detect the fax tone.
- The Cisco AS5400 Series Universal Gateways and Cisco AS5850 Universal Gateway have limitations on the number of ports that can run fax pass-through simultaneously.
- Fax pass-through is the state of the channel after the fax upspeed process has occurred. In fax pass-through mode, gateways do not distinguish a fax call from a voice call. Fax communication between the two fax machines is carried in its entirety in-band over a voice call. When using fax pass-through with upspeed, the gateways are to some extent aware of the fax call. Although relay mechanisms are not employed, with upspeed, the gateways recognize a called terminal identification fax tone, automatically change the voice codec to G.711 if necessary (thus the designation *upspeed*), and turn off echo cancellation and VAD for the duration of the call. Fax pass-through disables compression, echo cancellation, and issues redundant packets to ensure complete transmission.
- Fax pass-through is supported under these call control protocols:
  - H.323
  - SIP
  - Media Gateway Control Protocol (MGCP)

Modem Pass-Through

Modem pass-through over VoIP provides the transport of modem signals through a packet network by using PCM-encoded packets. It is based on the same logic as fax pass-through: An analog voice stream is encoded into G.711, passed through the network, and decoded back to analog signals at the far end.



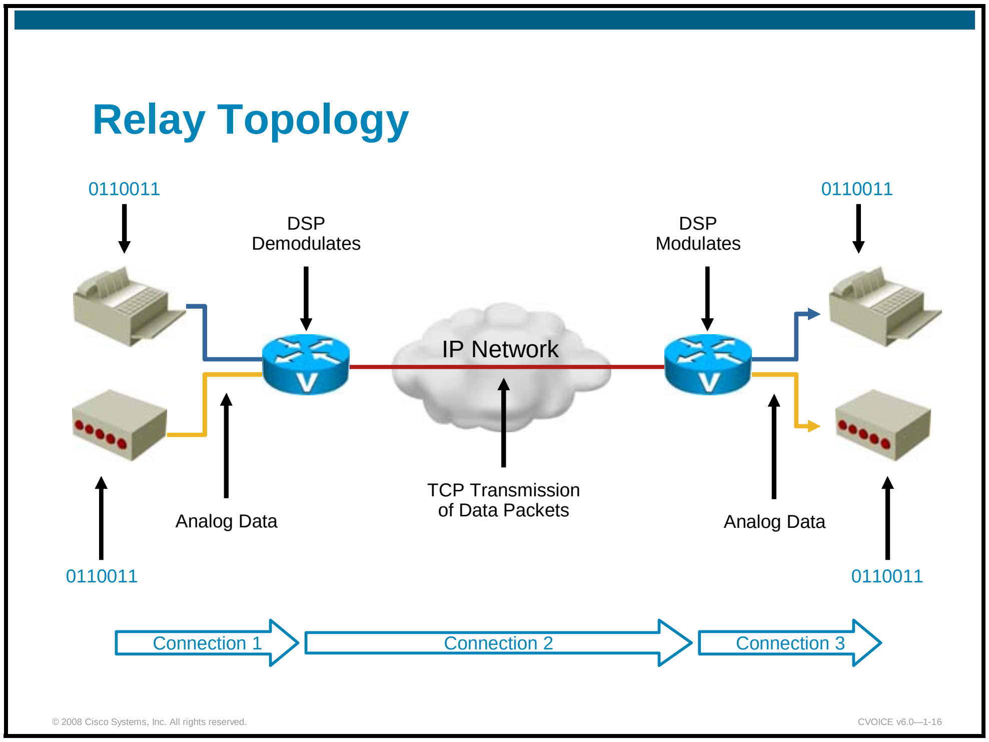
Modem Pass-Through Considerations

- Works only when the configured codec is G.711 or clear-channel.
- VAD and echo cancellation need to be disabled.
- Modem pass-through over VoIP performs these functions:
  - Represses processing functions
  - Issues redundant packets
  - Provides static jitter buffers
  - Differentiates modem signals from voice and fax signals
  - Reliably maintains a modem connection across the packet network

CVOICE v6.0—1-15

These factors need to be considered when determining whether to use modem pass-through:

- Modem pass-through does not support the switch from G.Clear to G.711.
- VAD and echo cancellation need to be disabled.
- Modem pass-through over VoIP performs these functions:
  - Represses processing functions like compression, echo cancellation, high-pass filter, and VAD
  - Issues redundant packets to protect against random packet drops
  - Provides static jitter buffers of 200 ms to protect against clock skew
  - Discriminates modem signals from voice and fax signals, indicating the detection of the modem signal across the connection and placing the connection in a state that transports the signal across the network with the least amount of distortion
  - Reliably maintains a modem connection across the packet network for a long duration under normal network conditions



Relay Topology

CVOICE v6.0—1-16

Fax Relay

Cisco fax relay is the default method for fax transmission on Cisco IOS gateways. It is an RTP-based transmission method that uses proprietary signaling and encoding mechanisms. Cisco fax relay capability is widely available and has been in Cisco IOS gateway software since Cisco IOS Release 11.3, which introduced DSPs to enable voice applications. In Cisco fax relay mode, gateways terminate T.30 fax signaling by spoofing a virtual fax machine to the locally attached fax machine. The mechanism for Cisco fax relay is the same for calls that are controlled by SIP, MGCP, and H.323 call control protocols.

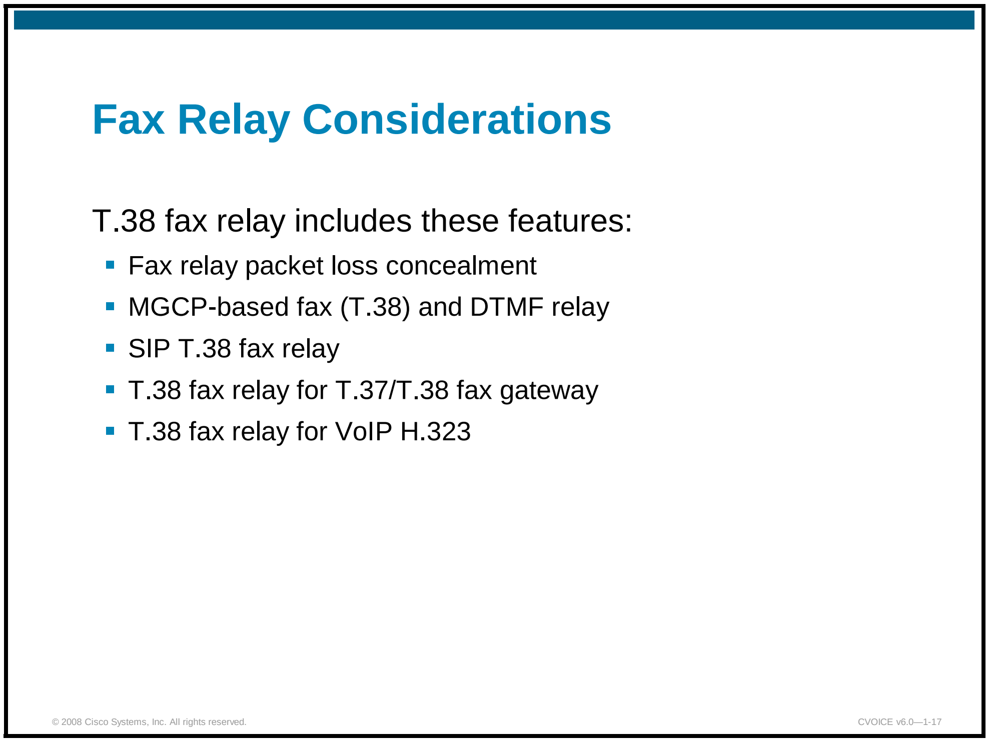
Note Before T.38 standards-based fax relay was introduced, no command-line interface (CLI) was required to enable Cisco fax relay.

Unlike fax pass-through, fax relay demodulates the fax bits at the local gateway, sends the information across the voice network using the fax relay protocol, and then remodulates the bits back into tones at the far gateway. The fax machines on either end are sending and receiving tones and are not aware that a demodulation/modulation fax relay process is occurring.

Cisco provides these two methods for fax relay:

- **Cisco fax relay:** A proprietary Cisco method and the default on most platforms if a fax method is not explicitly configured.
- **T.38 fax relay:** A method based on the ITU-T T.38 standard.T.38 fax relay. It is real-time fax transmission, that is, two fax machines are communicating with each other as if there were a direct phone line between them. T.38 fax relay is configured by using a few additional commands on gateway dial peers that have already been defined and configured for VoIP calls.

The T.38 fax relay feature can be configured for H.323, SIP, and MGCP call-control protocols. For H.323 and SIP networks, the only configuration tasks that differ are those involving the configuration of VoIP dial peers.



Fax Relay Considerations

T.38 fax relay includes these features:

- Fax relay packet loss concealment
- MGCP-based fax (T.38) and DTMF relay
- SIP T.38 fax relay
- T.38 fax relay for T.37/T.38 fax gateway
- T.38 fax relay for VoIP H.323

CVOICE v6.0—1-17

T.38 is an ITU-T standards-based method and protocol for fax relay. Data is packetized and encapsulated according to the T.38 standard. T.38 fax relay has these features:

- Fax relay PLC
- MGCP-based fax (T.38) and DTMF relay
- SIP T.38 fax relay
- T.38 fax relay for the T.37 or T.38 fax gateway
- T.38 fax relay for VoIP H.323

Modem Relay

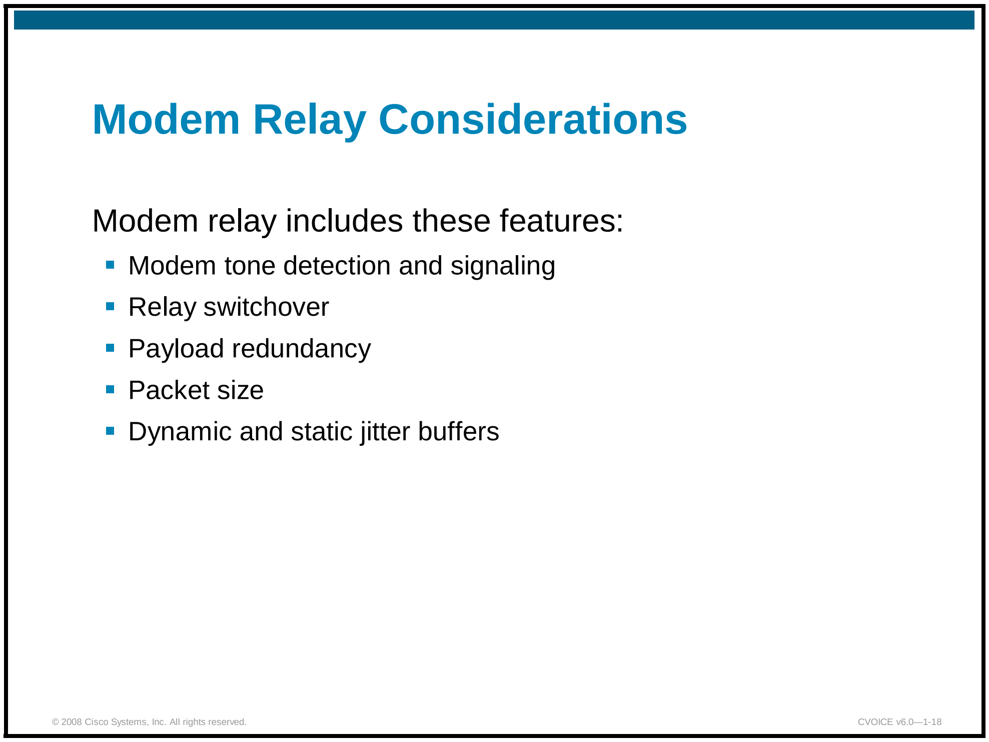
Cisco modem relay provides support for modem connections across traditional time-division multiplexing (TDM) networks. Modem relay demodulates a modem signal at one voice gateway and passes it as packet data to another voice gateway, where the signal is remodulated and sent to a receiving modem. On detection of the modem answer tone, the gateways switch into modem pass-through mode and then, if the call menu signal is detected, the two gateways switch into modem relay mode.

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

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

In this implementation, the call starts out as a voice call, and then switches into modem pass-through mode, and then into modem relay mode.

Modem relay significantly reduces the effects that dropped packets, latency, and jitter have on the modem session. Compared to modem pass-through, it also reduces the amount of bandwidth used.



Modem Relay Considerations

Modem relay includes these features:

- Modem tone detection and signaling
- Relay switchover
- Payload redundancy
- Packet size
- Dynamic and static jitter buffers

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-18

Modem relay includes these features:

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

Each of these features is described in more detail below.

Modem Tone Detection and Signaling

Modem relay supports V.34 modulation and the V.42 error correction and link layer protocol with maximum transfer rates of up to 33.6 kb/s. It forces higher-rate modems to train down to the supported rates. Signaling support includes SIP, MGCP or SGCP, and H.323:

- For MGCP and SIP, during the call setup, the gateways negotiate these items:
  - To use or not use the modem relay mode
  - To use or not use the gateway exchange identification (XID)
  - The value of the payload type for Named Signaling Event (NSE) packets
- For H.323, the gateways negotiate these items:
  - To use or not use the modem relay mode
  - To use or not use the gateway XID

Relay Switchover

When the gateways detect a data modem, both the originating gateway and the terminating gateway switch to modem pass-through mode by performing these actions:

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

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

Payload Redundancy

You can enable payload redundancy so that the modem pass-through over VoIP switchover causes the gateway to send redundant packets. Redundancy can be enabled in one or both of the gateways. When only a single gateway is configured for redundancy, the other gateway receives the packets correctly but does not produce redundant packets. When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

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

Dynamic and Static Jitter Buffers

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

Gateway-Controlled Modem Relay

Beginning with Cisco IOS Release 12.4(4)T, Cisco supports gateway-controlled negotiation parameters for modem relay. This new feature is a non-negotiated, bearer-switched mode for modem transport that does not involve call agent-assisted negotiation during the call setup. Instead, the negotiation parameters are configured directly on the gateway. These gateway-controlled negotiation parameters use NSEs to indicate the switchover from voice, to voice band data, to modem relay.

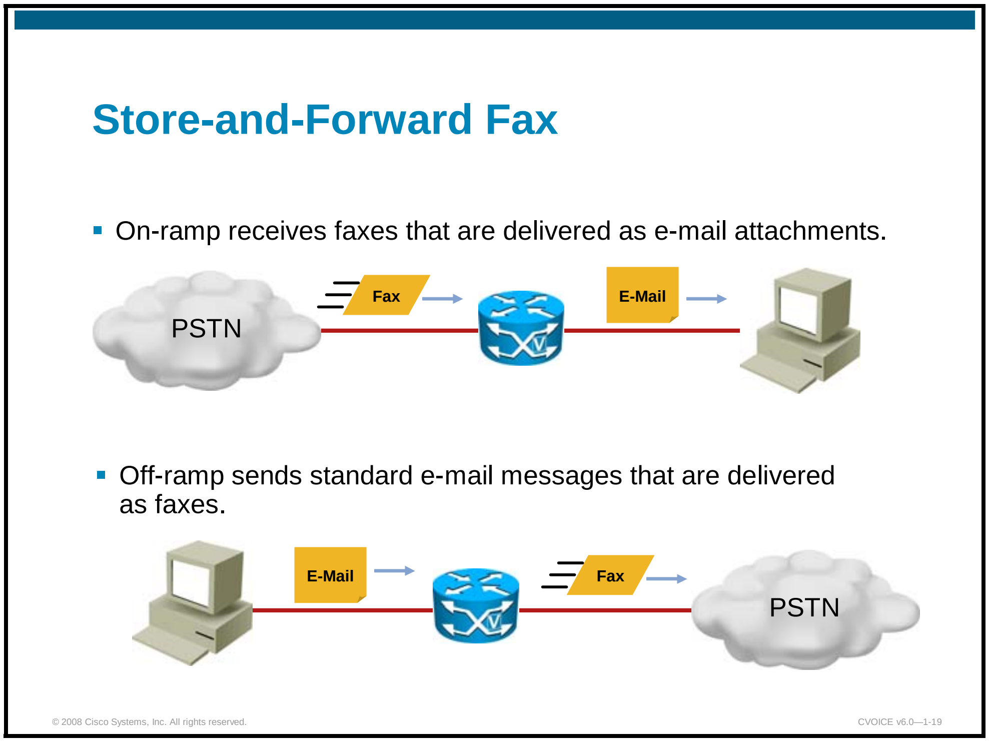
Upon detecting a 2100-Hz tone, the terminating gateway sends an NSE 192 to the originating gateway and switches over to modem pass-through. The terminating gateway also sends an NSE 199 to indicate modem relay. If this event is recognized by the originating gateway, the call occurs as modem relay. If the event is not recognized, the call occurs as modem pass-through.

Because Cisco modem relay uses configured parameters, it removes the signaling dependency from the call agent and allows modem relay support independent of call control. Cisco modem relay can be deployed over any call agent that is capable of setting up a voice connection between gateways, including Cisco Unified Communications Manager, Cisco Unified Communications Manager Express, and the Cisco BTS 10200 Softswitch and PGW 2200 Softswitch.

The gateway-controlled modem relay parameters are enabled by default when Cisco modem relay is configured, and when Cisco modem relay is configured, gateway XID parameter negotiation is always enabled. Gateway XID parameters are negotiated using the SPRT protocol.

Store-and-Forward Fax

This subtopic describes how the store-and-forward fax feature works.



Store-and-Forward Fax

- On-ramp receives faxes that are delivered as e-mail attachments.

- Off-ramp sends standard e-mail messages that are delivered as faxes.

CVOICE v6.0—1-19

The transmitting gateway is referred to as an "on-ramp gateway", and the terminating gateway is referred to as an "off-ramp gateway". Here's how they work:

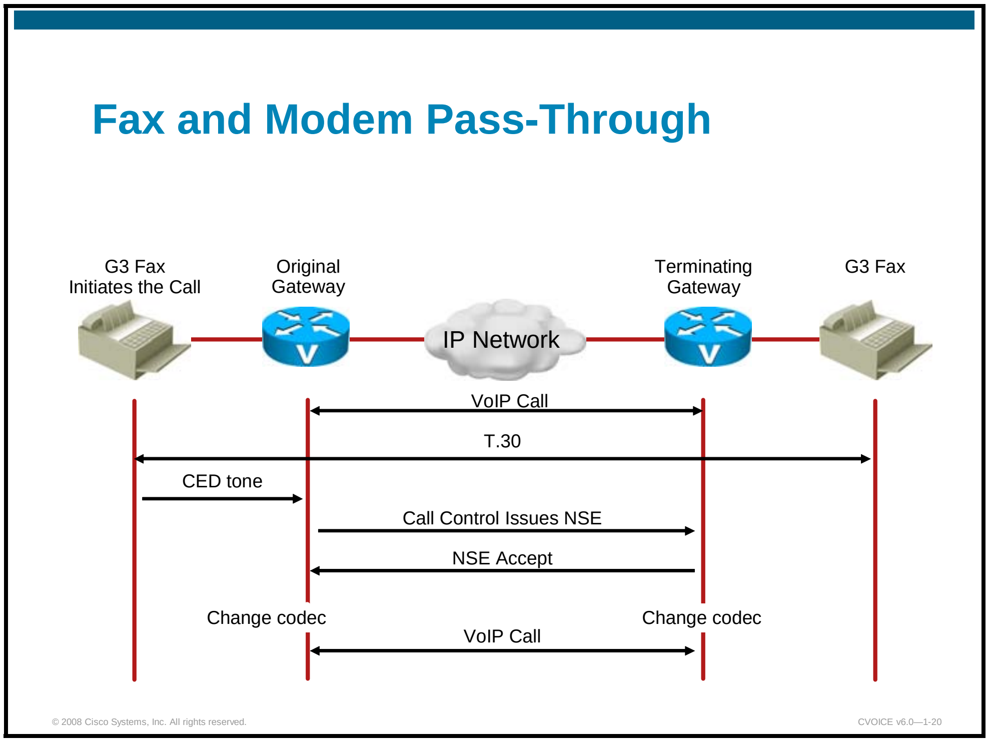
- **On-ramp faxing:** A voice gateway that handles incoming calls from a standard fax machine or the PSTN converts a traditional Group 3 (G3) fax to an e-mail message with a Tagged Image File Format (TIFF) attachment. The fax e-mail message and attachment are handled by an e-mail server while traversing the packet network and can be stored for later delivery or delivered immediately to a PC or to an off-ramp gateway.
- **Off-ramp faxing:** A voice gateway that handles calls going out from the network to a fax machine or the PSTN converts a fax e-mail with a TIFF attachment into a traditional fax format that can be delivered to a standard fax machine or the PSTN.

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

The basic functionality of store-and-forward fax is facilitated through Simple Mail Transfer Protocol (SMTP), with additional functionality that provides confirmation of delivery using existing SMTP mechanisms, such as Extended Simple Mail Transfer Protocol (ESMTP).

Gateway Signaling Protocols and Fax and Modem Pass-Through and Relay

This topic describes how T.38 and pass-through are supported by H.323, SIP, and MGCP.



Fax and Modem Pass-Through

CVOICE v6.0—1-20

The figure above illustrates a fax and modem pass-through operation. When a terminating gateway detects a called terminal identification (CED) tone from a called fax machine, the terminating gateway exchanges the voice codec that was negotiated during the voice call setup for a G.711 codec and turns off echo cancellation and VAD. This switchover is communicated to the originating gateway, which allows the fax machines to transfer modem signals as though they were traversing the PSTN. If the voice codec that was configured and negotiated for the VoIP call is G.711 when the CED tone is detected, there is no need to make any changes to the session other than turning off echo cancellation and VAD.

If pass-through is supported, these events occur:

1. For the duration of the call, the DSP listens for the 2100-Hz CED tone to detect a fax or modem on the line.

2. If the CED tone is heard, an internal event is generated to alert the call control stack that a fax or modem changeover is required.

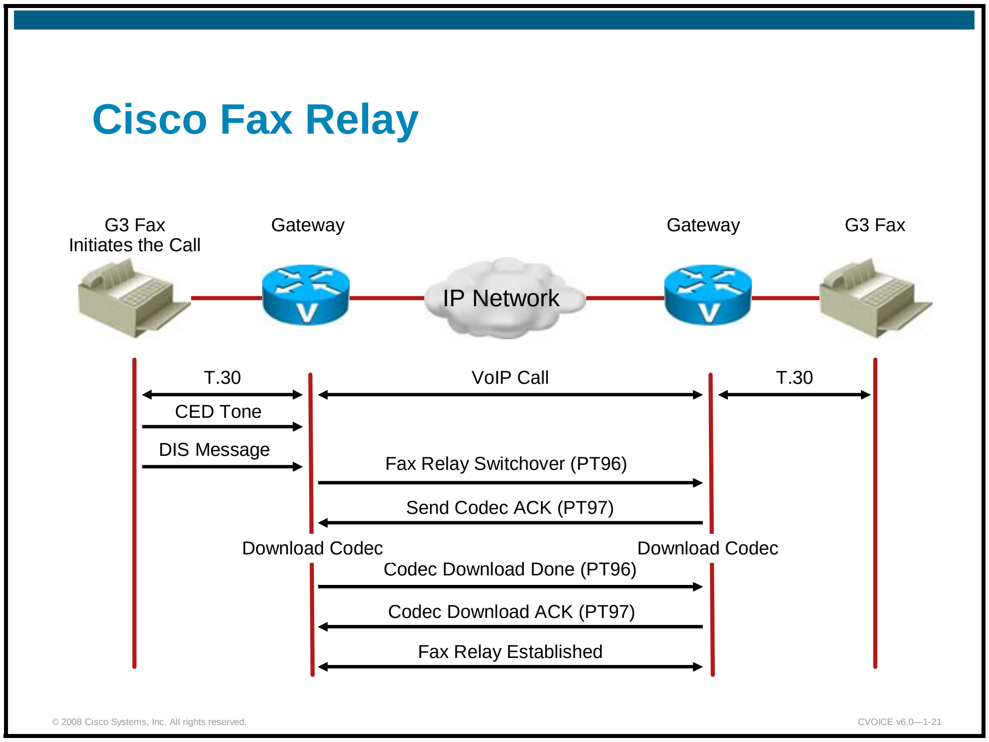
3. The call control stack on the originating gateway instructs the DSP to send a NSE to the terminating gateway, informing the terminating gateway of the request to carry out a codec change.

4. If the terminating gateway supports NSEs, it responds to the originating gateway instruction and loads the new codec. The fax machines are able to communicate on an end-to-end basis with no further intervention by the voice gateways.

Control of fax pass-through is achieved through NSEs that are sent in the RTP stream. NSEs are a proprietary Cisco version of IETF-standard named telephony events (NTEs), which are specially marked data packets used to digitally convey telephony signaling tones and events. NSEs use different event values than NTEs and are generally sent with RTP payload type 100, whereas NTEs use payload type 101. NSEs and NTEs provide a more reliable way to communicate tones and events by using a single packet rather than a series of in-band packets that can be corrupted or partially lost.

Fax pass-through and fax pass-through with upspeed use peer-to-peer NSEs within the RTP stream or bearer stream to coordinate codec switchover and the disabling of echo cancellation and VAD. Redundant packets can be sent to improve reliability when the probability of packet loss is high.

When a DSP is put into voice mode at the beginning of a VoIP call, the DSP is informed by the call control stack whether the control protocol can support pass-through or not.



Cisco Fax Relay

CVOICE v6.0—1-21

The figure illustrates a Cisco fax relay operation. When a DSP is put into voice mode at the beginning of a VoIP call, the DSP is informed by the call control stack whether fax relay is supported and if it is supported, whether it is Cisco fax relay or T.38 fax relay. If Cisco fax relay is supported, the following events occur:

1. Initially, a VoIP call is established as if it were a normal speech call. Call control procedures are followed and the DSP is put into voice mode, after which human speech is expected to be received and processed.

2. At any time during the life of the call, if a fax answer or calling tone (Answer back [ANSam] or CED) is heard, the DSP does not interfere with the speech processing. The ANSam or CED tone causes a switch to modem pass-through, if enabled, to allow the tone to pass cleanly to the remote fax.

3. A normal fax machine, after generating a CED or hearing a calling (CNG) tone, sends a digital information signal (DIS) message with the capabilities of the fax machine. The DSP in the Cisco IOS gateway attached to the fax machine that generated the DIS message (normally the terminating gateway) detects the High-Level Data Link Control (HDLC) flag sequence at the start of the DIS message and initiates fax relay switchover. The DSP also triggers an internal event to notify the call control stack that fax switchover is required. The call control stack then instructs the DSP to change the RTP payload type to 96 and to send this payload type to the originating gateway.

4. When the DSP on the originating gateway receives an RTP packet with the payload type set to 96, it triggers an event to inform its own call control stack that a fax changeover has been requested by the remote gateway. The originating gateway then sends an RTP packet to the terminating gateway with payload type 97 to indicate that the originating gateway has started the fax changeover. When the terminating gateway receives the payload type 97 packet, the packet serves as an acknowledgement. The terminating gateway starts the fax codec download and is ready for fax relay.

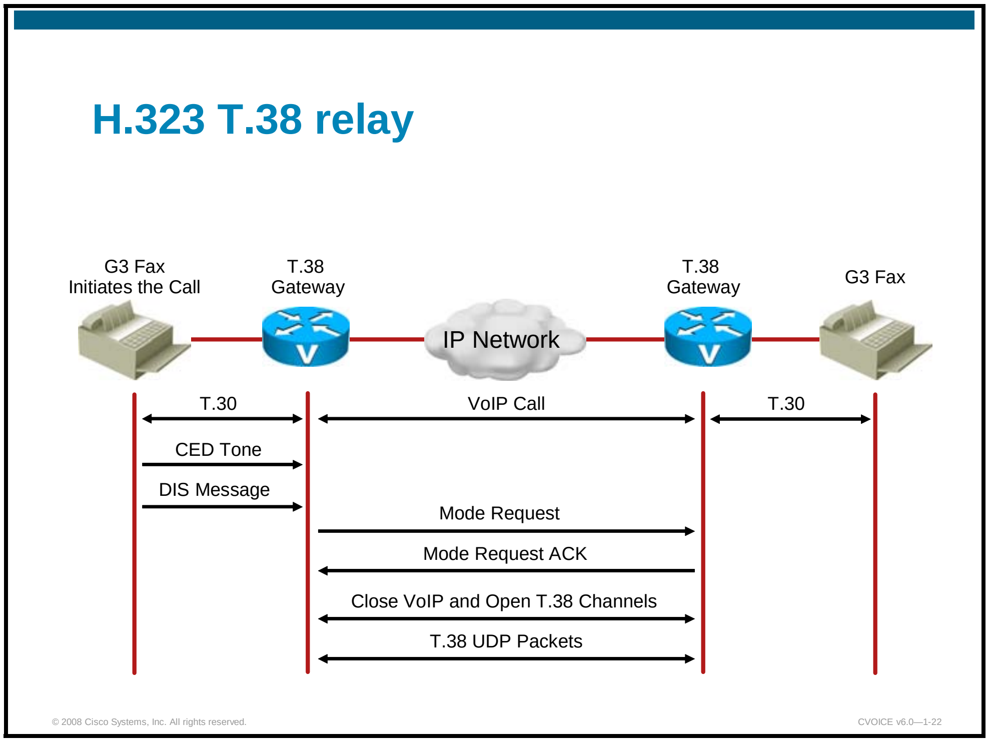
5. Once the originating gateway has completed the codec download, it sends RTP packets with payload type 96 to the terminating gateway. The terminating gateway responds with an RTP packet with payload type 97, and fax relay can begin between the two gateways. As part of the fax codec download, other parameters such as VAD, jitter buffers, and echo cancellation are changed to suit the different characteristics of a fax call.

During fax relay operation, the T.30 analog fax signals are received from the PSTN or from a directly attached fax machine. The T.30 fax signals are demodulated by a DSP on the gateway and then packetized and sent across the VoIP network as data. The terminating gateway decodes the data stream and remodulates the T.30 analog fax signals to be sent to the PSTN or to a destination fax machine.

The messages that are demodulated and remodulated are predominantly the phase B, phase D, and phase E messages of a T.30 transaction. Most of the messages are passed across without any interference, but certain messages are modified according to the constraints of the VoIP network.

During phase B, each fax machine interrogates the capabilities of the other. They expect to communicate with each other across a 64-kb/s PSTN circuit, and they attempt to make best use of the available bandwidth and circuit quality of a 64-kb/s voice path. However, in a VoIP network, the fax machines do not have a 64-kb/s PSTN circuit available. The bandwidth per call is probably less than 64 kb/s, and the circuit is not considered a clear circuit.

Because transmission paths in VoIP networks are more limited than in the PSTN, Cisco IOS CLI is used to adjust fax settings on the VoIP dial peer. The adjusted fax settings restrict the facilities that are available to fax machines across the VoIP call leg and are also used to modify values in DIS and NSF messages that are received from fax machines.



H.323 T.38 relay

CVOICE v6.0—1-22

The figure illustrates an H.323 T.38 relay operation. The T.38 fax relay feature provides an ITU-T standards-based method and protocols for fax relay. Data is packetized and encapsulated according to the T.38 standard. The encoding of the packet headers and the mechanism to switch from VoIP mode to fax relay mode are clearly defined in the specification. Annexes to the basic specification include details for operation under SIP and H.323 call control protocols.

Here is the H.245 message flow:

1. Initially, a VoIP call is established as if it were a normal speech call. Call control procedures are followed and the DSP is put into voice mode, after which human speech is expected to be received and processed.

2. At any time during the life of the call, if a fax answer or calling tone (ANSam or CED) is heard, the DSP does not interfere with the speech processing. The ANSam or CED tone causes a switch to modem pass-through, if enabled, to allow the tone to pass cleanly to the remote fax.

3. A normal fax machine, after generating a CED or hearing a CNG, sends a DIS message with the capabilities of the fax machine. The DSP in the Cisco IOS gateway attached to the fax machine that generated the DIS message (normally the terminating gateway) detects the HDLC flag sequence at the start of the DIS message and initiates fax relay switchover. The DSP also triggers an internal event to notify the call control stack that fax switchover is required. The call control stack then instructs the DSP to change the RTP payload type to 96 and to send this payload type to the originating gateway.

4. The detecting terminating gateway sends a ModeRequest message to the originating gateway, and the originating gateway responds with a ModeRequestAck.

5. The originating gateway sends a closeLogicalChannel message to close its VoIP UDP port, and the terminating gateway responds with a closeLogicalChannelAck message while it closes the VoIP port.

6. The originating gateway sends an openLogicalChannel message that indicates to which port to send the T.38 UDP information on the originating gateway, and the terminating gateway responds with an openLogicalChannelAck message.

7. The terminating gateway sends a closeLogicalChannel message to close its VoIP UDP port, and the originating gateway responds with a closeLogicalChannelAck message.

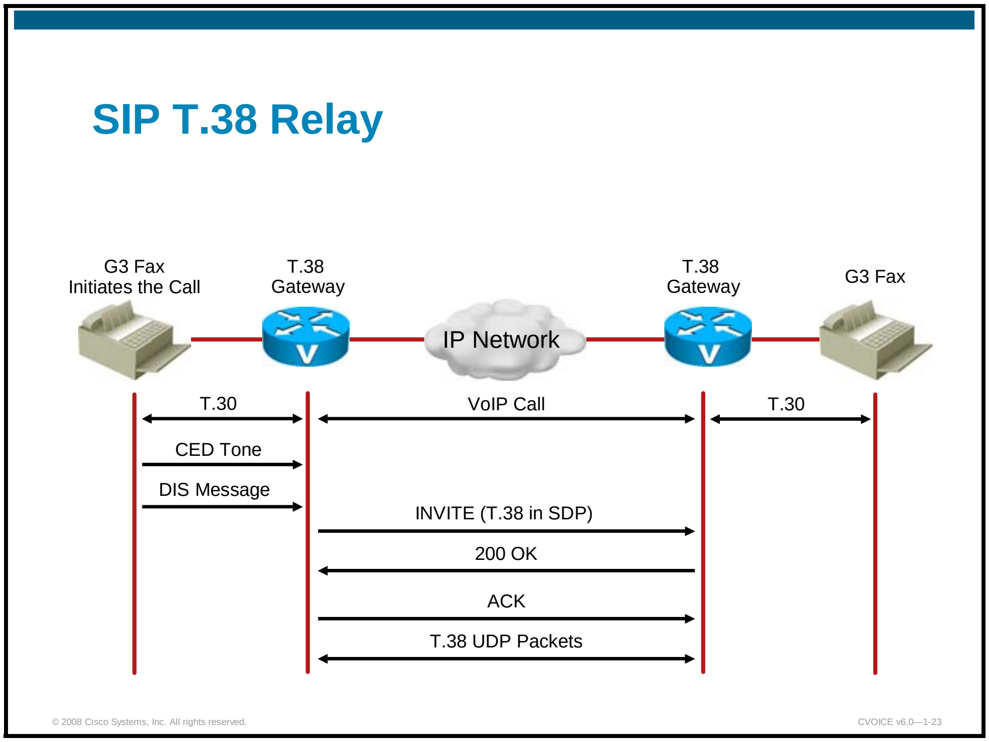
8. The terminating gateway sends an openLogicalChannel message that indicates to which port to send the T.38 UDP stream, and the originating gateway responds with an openLogicalChannelAck message.

9. T.38-encoded UDP packets flow back and forth. At the end of the fax transmission, either gateway can initiate another ModeRequest message to return to VoIP mode.

T.38 fax relay uses data redundancy to accommodate packet loss. During T.38 call establishment, voice gateways indicate the level of packet redundancy that they incorporate in their transmission of fax UDP transport layer packets. The level of redundancy (the number of times that the packet is repeated) can be configured on Cisco IOS gateways.

The T.38 Annex B standard defines the mechanism that is used to switch over from voice mode to T.38 fax mode during a call. The ability to support T.38 must be indicated during the initial VoIP call setup. If the DSP on the gateway is capable of supporting T.38 mode, this information is indicated during the H.245 negotiation procedures as part of the regular H.323 VoIP call setup.

After the VoIP call setup is completed, the DSP continues to listen for a fax tone. When a fax tone is heard, the DSP signals the receipt of fax tone to the call control layer, which then initiates fax changeover as specified in the T.38 Annex B procedures.



SIP T.38 Relay

CVOICE v6.0—1-23

When SIP is the call control protocol, T.38 Annex D procedures are used for the changeover from VoIP to fax mode during a call. Initially, a normal VoIP call is established using SIP INVITE messages. The DSP needs to be informed that it can support T.38 mode while it is put into voice mode. Then, during the call, when the DSP detects fax HDLC flags, it signals the detection of the flags to the call control layer, and the call control layer initiates a SIP INVITE message midcall to signal the desire to change the media stream.

Here is the SIP T.38 fax relay call flow:

1. Initially, a VoIP call is established as if it were a normal speech call. Call control procedures are followed and the DSP is put into voice mode, after which human speech is expected to be received and processed.

2. At any time during the life of the call, if a fax answer or calling tone (ANSam or CED) is heard, the DSP does not interfere with the speech processing. The ANSam or CED tone causes a switch to modem pass-through, if enabled, to allow the tone to pass cleanly to the remote fax.

3. A normal fax machine, after generating a CED or hearing a CNG, sends a DIS message with the capabilities of the fax machine. The DSP in the Cisco IOS gateway attached to the fax machine that generated the DIS message (normally the terminating gateway) detects the HDLC flag sequence at the start of the DIS message and initiates fax relay switchover. The DSP also triggers an internal event to notify the call control stack that fax switchover is required. The call control stack then instructs the DSP to change the RTP payload type to 96 and to send this payload type to the originating gateway.

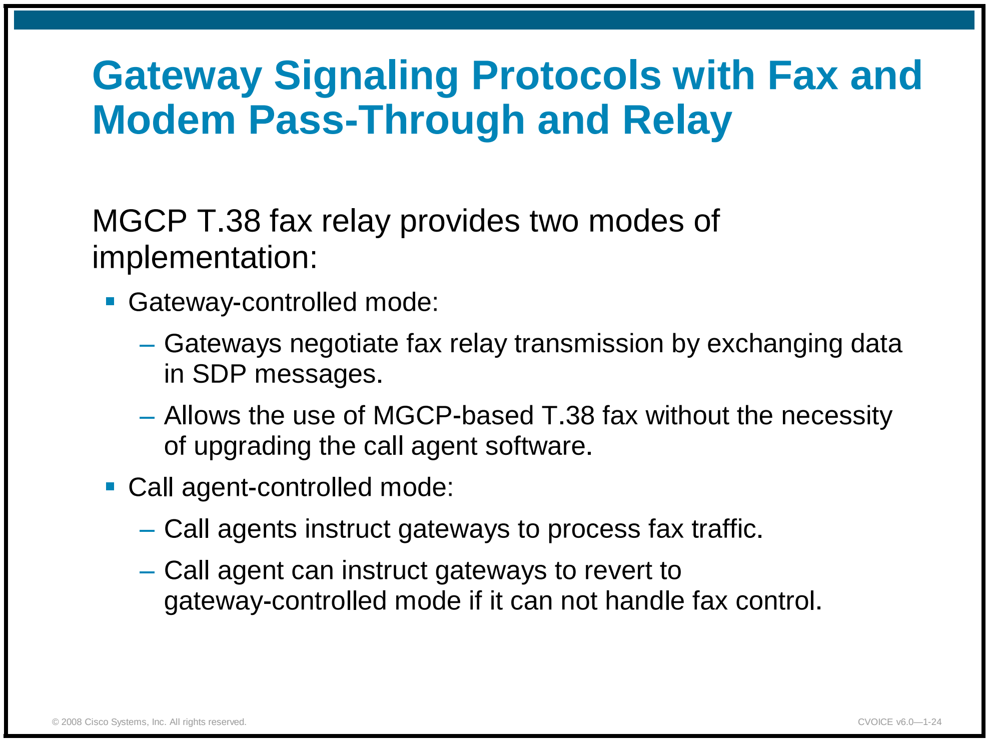
4. The terminating gateway detects a fax V.21 flag sequence and sends an INVITE message with T.38 details in the SDP field to the originating gateway or to the SIP proxy server, depending on the network topology.

5. The originating gateway receives the INVITE message and sends back a 200 OK message.

6. The terminating gateway acknowledges the 200 OK message and sends an ACK message directly to the originating gateway.

7. The originating gateway starts sending T.38 UDP packets instead of VoIP UDP packets across the same ports.

8. At the end of the fax transmission, another INVITE message can be sent to return to VoIP mode.



Gateway Signaling Protocols with Fax and Modem Pass-Through and Relay

MGCP T.38 fax relay provides two modes of implementation:

- Gateway-controlled mode:
  - Gateways negotiate fax relay transmission by exchanging data in SDP messages.
  - Allows the use of MGCP-based T.38 fax without the necessity of upgrading the call agent software.
- Call agent-controlled mode:
  - Call agents instruct gateways to process fax traffic.
  - Call agent can instruct gateways to revert to gateway-controlled mode if it can not handle fax control.

CVOICE v6.0—1-24

The MGCP T.38 fax relay feature conforms to ITU-T T.38, “Procedures for Real-Time Group 3 Facsimile Communication over IP Networks,” which determines procedures for real-time fax communication in various External Gateway Control Protocol (XGCP) applications.

MGCP T.38 fax relay provides two modes of implementation:

- **Gateway-controlled mode:** Gateways negotiate fax relay transmission by exchanging capability information in Session Description Protocol (SDP) messages. Transmission of SDP messages is transparent to the call agent. Gateway-controlled mode allows the use of a MGCP-based T.38 fax without the necessity of upgrading the call agent software to support the feature.
- **Call agent-controlled mode:** Call agents use MGCP messaging to instruct gateways to process fax traffic. For MGCP T.38 fax relay, call agents can also instruct gateways to revert to gateway-controlled mode if the call agent is unable to handle the fax control messaging traffic, as is the case in overloaded or congested networks.

MGCP-based T.38 fax relay enables interworking between the T.38 application that already exists on Cisco gateways and the MGCP applications on call agents.

Here is the call flow for an MGCP-based T.38 fax relay:

1. A call is initially established as a voice call.
2. The gateways advertise capabilities in an SDP exchange during connection establishment.
3. If both gateways do not support T.38 fax relay, fax pass-through is used for fax transmission. If both gateways support T.38, they attempt to switch to T.38 upon fax tone detection. The existing audio channel is used for T.38 fax relay, and the existing connection port is reused to minimize delay. If failure occurs at some point during the switch to T.38, the call reverts to the original settings it had as a voice call. If this failure occurs, a fallback to fax pass-through is not supported.

4. Upon completion of the fax image transfer, the connection remains established and reverts to a voice call using the previously designated codec, unless the call agent instructs the gateways to do otherwise.

A fax relay MGCP event allows the gateway to notify the call agent of the status (start, stop, or failure) of T.38 processing for the connection. This event is sent in both call agent-controlled and gateway-controlled mode.

Gateway-Controlled MGCP T.38 Fax Relay

In gateway-controlled mode, a call agent uses the fx: extension of the local connection option (LCO) to instruct a gateway about how to process a call. Gateways do not need instruction from the call agent to switch to T.38 mode. This mode is used if the call agent has not been upgraded to support T.38 and MGCP interworking, or if the call agent does not want to manage fax calls. Gateway-controlled mode can also be used to bypass the message delay overhead caused by call agent handling, for example, to meet time requirements for switchover to T.38 mode. If the call agent does not specify the mode to the gateway, the gateway defaults to gateway-controlled mode.

In gateway-controlled mode, the gateways exchange NSEs by performing these actions:

- Instruct the peer gateway to switch to T.38 for a fax transmission.
- Either acknowledge the switch and the readiness of the gateway to accept T.38 packets or indicate that the gateway cannot accept T.38 packets.

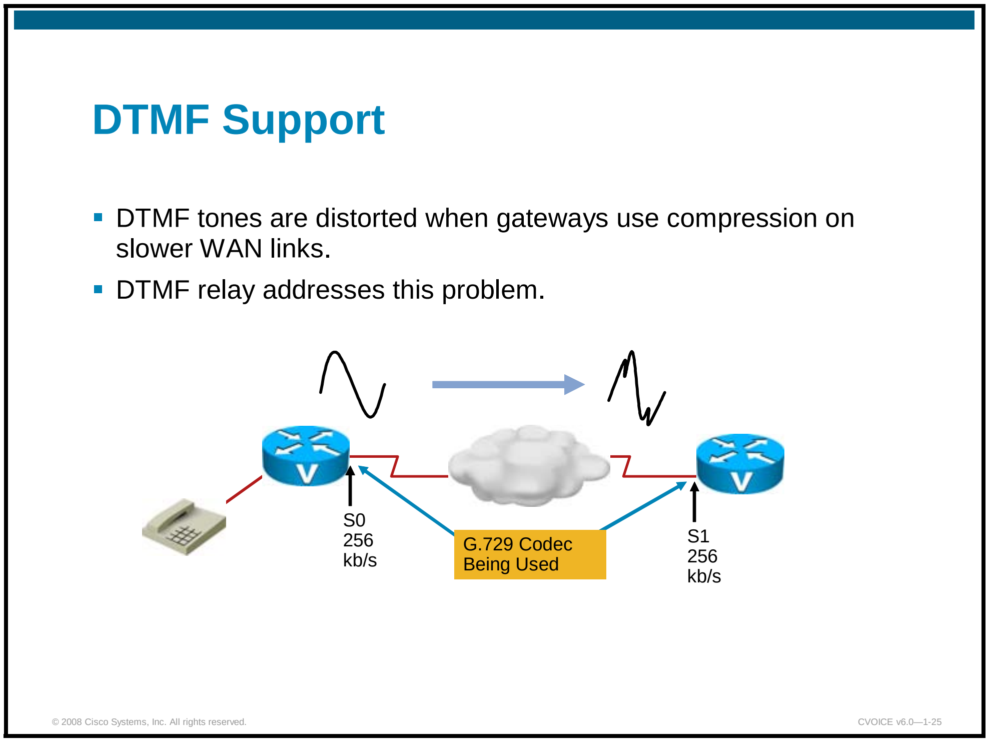
Call Agent-Controlled MGCP T.38 Fax Relay

In call agent-controlled mode, the call agent can instruct the gateway to switch to T.38 for a call. In Cisco IOS Release 12.3(1) and later releases, call agent-controlled mode enables T.38 fax relay interworking between H.323 gateways and MGCP gateways and between two MGCP gateways under the control of a call agent. This feature supersedes previous methods for call agent-controlled fax relay and introduces these gateway capabilities:

- Ability to accept the MGCP FXR package, to receive the fxr prefix in commands from the call agent, and to send the fxr prefix in notifications to the call agent.
- Ability to accept a new port when the gateway is switching from voice to fax transmission during a call. This new ability allows successful T.38 call agent-controlled fax communications between H.323 and MGCP gateways in those situations in which the H.323 gateway assigns a new port when it is changing a call from voice to fax. New ports are assigned in H.323 gateways using images from Cisco IOS Release 12.2(2)T to Cisco IOS Release 12.2(7.5)T. (MGCP gateways in MGCP-to-MGCP fax calls simply reuse the same port, but call agent-controlled T.38 fax relay enables MGCP gateways to handle both situations, either switching to a new port or reusing the same port, as directed by the call agent.)

DTMF Support

This topic describes DTMF relay and how it is supported in MGCP, H323, and SIP.



DTMF Support

- DTMF tones are distorted when gateways use compression on slower WAN links.
- DTMF relay addresses this problem.

Dual tone multifrequency (DTMF) is the tone generated on a touchtone phone when the keypad digits are pressed. Gateways send these tones in the RTP stream by default. This default behavior is fine when the voice stream is sent uncompressed, but problems arise when gateways use compression algorithms to send voice across slower WAN links.

During a call, DTMF may be entered to access IVR systems such as voice mail and automated banking services. Although DTMF is usually transported accurately when high-bit-rate voice codecs such as G.711 are being used, low-bit-rate codecs such as G.729 and G.723.1 are highly optimized for voice patterns and tend to distort DTMF tones. As a result, IVR systems may not correctly recognize the tones.

DTMF relay solves the problem of DTMF distortion by transporting DTMF tones “out of band,” or separate from the RTP voice stream.

H.323 DTMF Support

Cisco gateways currently support four methods of DTMF relay using H.323:

- **Proprietary Cisco:** DTMF tones are sent in the same RTP channel as voice data. However, the DTMF tones are encoded differently from the voice samples and are identified as payload type 121, which enables the receiver to identify them as DTMF tones. This method requires the use of Cisco gateways at both the originating and terminating endpoints of the H.323 call.
- **H.245 alphanumeric:** Separates the DTMF digits from the voice stream and sends them through the H.245 signaling channel instead of through the RTP channel. The tones are transported in H.245 User Input Indication messages. The H.245 signaling channel is a

reliable channel, so the packets that transport the DTMF tones are guaranteed to be delivered. This method does not send tone length information.

Note All H.323 version 2-compliant systems are required to support the H.245 alphanumeric method, while support of the H.245 signal method is optional.

- **H.245 signal:** This method does pass along tone length information, thereby addressing a potential problem with the alphanumeric method. This method is optional on H.323 gateways.
- **NTEs:** Transports DTMF tones in RTP packets according to Section 3 of RFC 2833. RFC 2833 defines formats of NTE RTP packets that are used to transport DTMF digits, hookflash, and other telephony events between two peer endpoints. With the NTE method, the endpoints perform per-call negotiation of the DTMF relay method. They also negotiate to determine the payload type value for the NTE RTP packets. User preference for DTMF relay types is not supported, and DTMF relay forking is not supported.

MGCP DTMF Support

These are the four current implementations of MGCP-based DTMF relay:

- **Proprietary Cisco:** DSPs on the gateways send and receive DTMF digits in-band in the voice RTP stream but codes them differently so they can be identified by the receiver as DTMF tones.
- **NSE:** Conforms to RFC 2833 to provide a standardized method of DTMF transport using NTEs in RTP packets. RFC 2833 support is standards-based and allows greater interoperability with other gateways and call agents.
- **NTE:** Provides for two modes of implementation:
  - **Gateway-controlled mode:** In gateway-controlled mode, the gateways negotiate DTMF transmission by exchanging capability information in SDP messages. That transmission is transparent to the call agent. Gateway-controlled mode allows the use of the DTMF relay feature without upgrading the call agent software to support the feature.
  - **Call agent-controlled mode:** In call agent-controlled mode, call agents use MGCP messaging to instruct gateways to process DTMF traffic.
- **Out-of-band:** Sends the tones as signals to the Cisco Unified Communications Manager out-of-band over the control channel. Cisco Unified Communications Manager interprets the signals and passes them on.

SIP DTMF Support

SIP gateways can use Cisco proprietary NOTIFY-based out-of-band DTMF relay. In addition, NOTIFY-based out-of-band DTMF relay can also be used by analog phones attached to analog voice ports (known as a Foreign Exchange Station, or FXS) on the router.

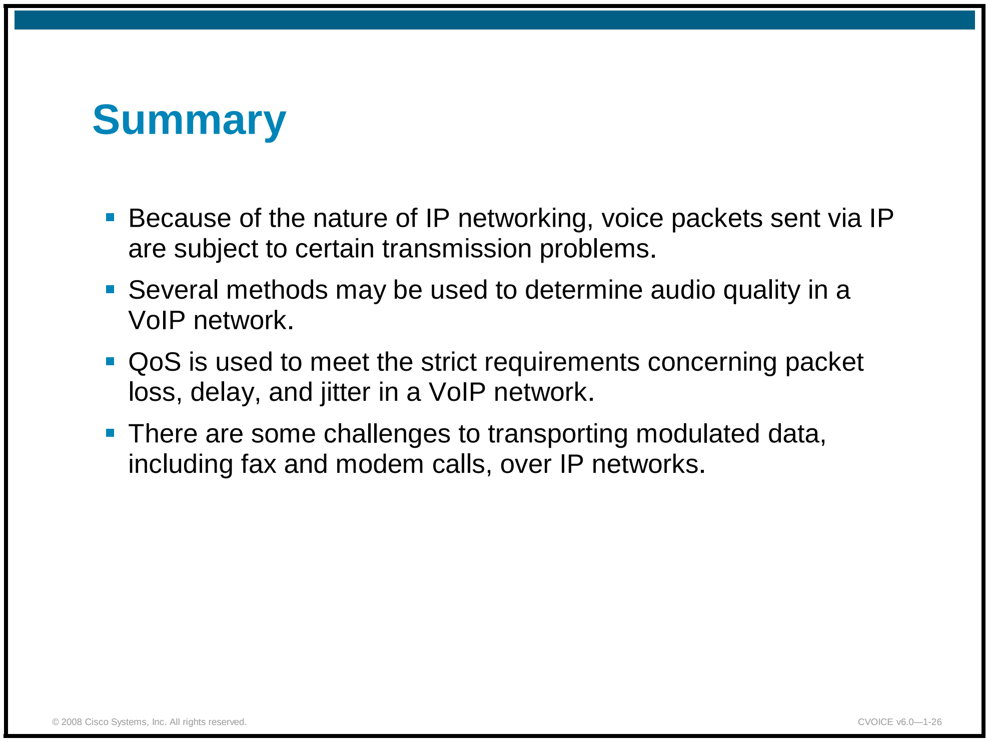
NOTIFY-based out-of-band DTMF relay sends messages bidirectionally between the originating and terminating gateways for a DTMF event during a call. If multiple DTMF relay mechanisms are enabled on a SIP dial peer and are negotiated successfully, NOTIFY-based out-of-band DTMF relay takes precedence.

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

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

Summary

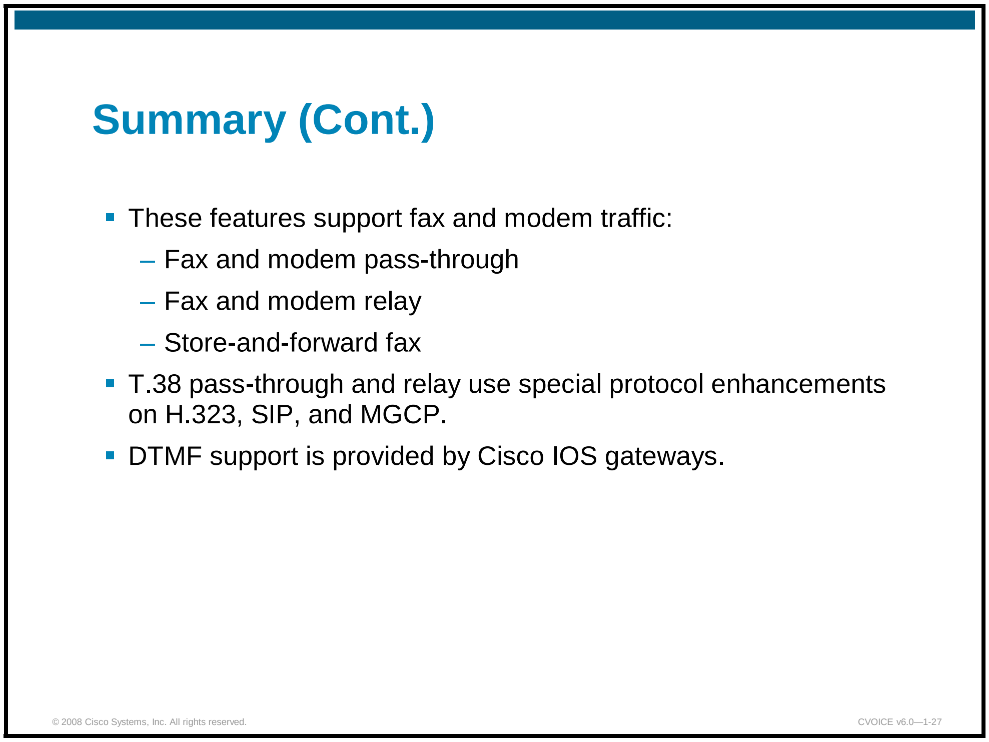
This topic summarizes the key points that were discussed in this lesson.



Summary

- Because of the nature of IP networking, voice packets sent via IP are subject to certain transmission problems.
- Several methods may be used to determine audio quality in a VoIP network.
- QoS is used to meet the strict requirements concerning packet loss, delay, and jitter in a VoIP network.
- There are some challenges to transporting modulated data, including fax and modem calls, over IP networks.

CVOICE v6.0—1-26



Summary (Cont.)

- These features support fax and modem traffic:
  - Fax and modem pass-through
  - Fax and modem relay
  - Store-and-forward fax
- T.38 pass-through and relay use special protocol enhancements on H.323, SIP, and MGCP.
- DTMF support is provided by Cisco IOS gateways.

CVOICE v6.0—1-27

Lesson Self-Check

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

Q1) Jitter is defined as a variation in the _____ of received packets.

Relates to: IP Networking and Audio Clarity

Q2) Two methods that may be used to determine signal quality are _____ and _____.

Relates to: Audio Quality Measurement

Q3) Network administrators use ________ to meet the strict requirements concerning packet loss, delay, and delay variation in a VoIP network.

Relates to: VoIP and QoS

Q4) The three conceptual methods of carrying virtual real-time fax machine–to–fax machine communications across packet networks are fax _____, _____, and _____.

Relates to: Transporting Modulated Data over IP Networks

Q5) Fax _____ is the simplest technique for sending fax over IP networks.

Relates to: Understanding Fax and Modem Pass-Through, Relay, and Store and Forward

Q6) Control of fax pass-through is achieved through _____ that are sent in the RTP stream.

Relates to: Gateway Signaling Protocols and Fax and Modem Pass-Through and Relay

Q7) The tone that is generated on a touchtone phone when the keypad digits are pressed is called _____.

Relates to: DTMF Support

Lesson Self-Check Answer Key

Q1) delay

Q2) MOS, PESQ

Q3) QoS

Q4) pass-through, relay, store-and-forward

Q5) pass-through

Q6) NSEs

Q7) DTMF

Lesson 4

Understanding Codecs, Codec Complexity, and DSP Functionality

Overview

Because WAN bandwidth is probably the most expensive component of an enterprise network, network administrators must know how to calculate the total bandwidth that is required for voice traffic and how to reduce overall consumption. This lesson describes in detail coder-decoders (codecs), digital signal processors (DSPs), codec complexity, and the bandwidth requirements for VoIP calls. Several variables affecting total bandwidth are explained, as is the method of calculating and reducing total bandwidth.

Objectives

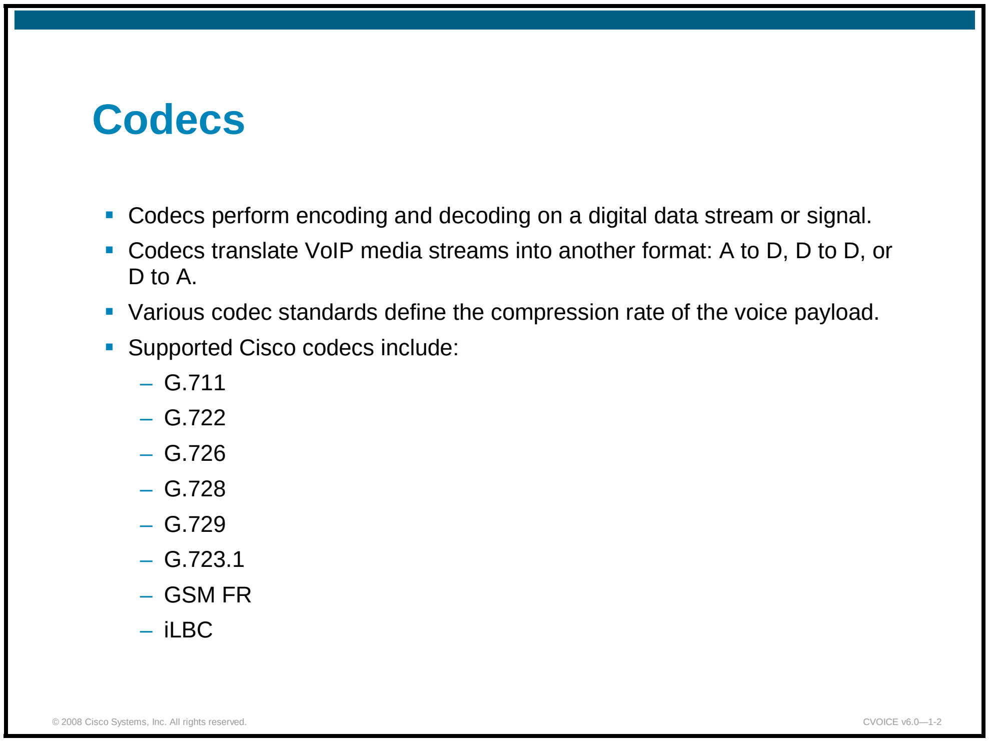
Upon completing this lesson, you will be able to describe various codecs, how to configure codec complexity, and how DSPs are used as media resources. This ability includes being able to meet these objectives:

- Describe various codecs and their bandwidth requirements
- Describe how the number of voice samples that are encapsulated impacts bandwidth requirements
- Calculate the overhead for Layer 2 and other protocols on a VoIP call
- Use a formula to calculate the total bandwidth that is required for a VoIP call with and without VAD
- Describe various types of DSPs, DSP functions, and how DSPs are used as media resources
- Describe codec complexity and where and how to configure it
- Describe the DSP requirements for various media resources and calculate the actual number of DSPs required
- Describe DSP farms, DSP farm profiles, and how to configure conferencing and transcoding on a voice gateway

- Describe the commands that are required to configure DSP farms on Cisco IOS gateways for enhanced media resources
- Describe how to verify the correct operation of available media resources

Codecs

This topic describes various codecs and their bandwidth requirements.



Codecs

- Codecs perform encoding and decoding on a digital data stream or signal.
- Codecs translate VoIP media streams into another format: A to D, D to D, or D to A.
- Various codec standards define the compression rate of the voice payload.
- Supported Cisco codecs include:
  - G.711
  - G.722
  - G.726
  - G.728
  - G.729
  - G.723.1
  - GSM FR
  - iLBC

CVOICE v6.0—1-2

A codec is a device or program capable of performing encoding and decoding on a digital data stream or signal. Various types of codecs are used to encode and decode or compress and decompress various types of data that would otherwise use up large amounts of bandwidth on WAN links. Codecs are especially important on low-speed serial links where every bit of bandwidth is needed and utilized to ensure network reliability.

Proper capacity planning is one of the most important factors for network administrators to consider while they are building voice networks. Network administrators must understand how much bandwidth is used for each VoIP call. In order to understand bandwidth, the administrator must know which codec is being utilized across the WAN link. With a thorough understanding of VoIP bandwidth and codecs, the network administrator can apply capacity-planning tools.

Coding techniques are standardized by the ITU. The ITU G-series codecs are among the most popular standards for VoIP applications.

Following is a list of codecs supported by the Cisco IOS gateways:

- **G.711:** Is the international standard for encoding telephone audio on a 64-kb/s channel. It is a pulse code modulation (PCM) scheme operating at an 8-kHz sample rate, with 8 bits per sample. With G.711, the encoded voice is already in the correct format for digital voice delivery in the public switched telephone network (PSTN) or through PBXs. It is widely used in the telecommunications field because it improves the signal-to-noise ratio without increasing the amount of data.

There are two subsets of the G.711 codec:

- **mu-law:** Mu-law is used in North American and Japanese phone networks.
- **a-law:** A-law is used in Europe and elsewhere around the world.

Both mu-law and a-law subsets use compressed speech carried in 8-bit samples. They use an 8-kHz sampling rate with 64 kb/s of storage.

- **G.722:** Is an ITU standard wideband speech codec that provides 7 kHz of wideband audio at data rates from 48 to 64 kb/s. Technology of the codec is based on split band adaptive differential PCM (ADPCM). G.722.1 offers lower bit-rate compressions. A more recent variant, G.722.2, also known as Adaptive Multi-Rate Wideband (AMR-WB), offers even lower bit-rate compressions as well as the ability to quickly adapt to varying compressions as the network topography mutates. In the latter case, bandwidth is automatically conserved when network congestion is high. When congestion returns to a normal level, a lower-compression, higher-quality bit rate is restored. G.722 is the original 7-kHz codec, using ADPCM and operating at 48 to 64 kb/s. G.722.1 operates at half the data rate while delivering comparable or better quality than G.722, but it is a transform-based codec. And G.722.2, which operates on wideband speech and delivers very low bit rates, is a code-excited linear prediction (CELP)-based algorithm. G.722 and its variants sample audio data at a rate of 16 kHz, double that of traditional telephony interfaces, which results in superior audio quality and clarity.
- **G.726:** Is an ITU-T ADPCM coding that operates at data rates of 40, 32, 24, and 16 kb/s. ADPCM-encoded voice can be interchanged between packet voice, PSTN, and PBX networks if the PBX networks are configured to support ADPCM. The four bit rates associated with G.726 are often referred to by the bit size of a sample, which are 2-bits, 3-bits, 4-bits, and 5-bits respectively.
- **G.728:** Describes a 16-kb/s low-delay CELP (LD-CELP) variation of CELP voice compression. CELP voice coding must be translated into a public telephony format for delivery to or through the PSTN.
- **G.729:** Uses conjugate-structure algebraic-CELP (CS-ACELP) compression to code voice into 8-kb/s streams. There are two variations of this standard (G.729 and G.729 Annex A [G.729A]) that differ mainly in computational complexity. G.729A requires less computation, but the lower complexity is not free because speech quality is marginally worsened. Standard G.729 operates at 8 kb/s, but there are extensions, which also provide 6.4 kb/s (Annex D) and 11.8 kb/s (Annex E) rates for marginally worse and better speech quality respectively.
- **G.723:** Describes a dual-rate speech coder for multimedia communications. This compression technique can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards. This codec has two bit rates associated with it:

  - **r63:** 6.3 kb/s; using 24 byte frames and the Multipulse LPC with Maximum Likelihood Quantization (MPC-MLQ) algorithm
  - **r53:** 5.3 kb/s; using 20 byte frames and the ACELP algorithm

  The higher bit rate is based on MPC-MLQ technology and provides a somewhat higher quality of sound. The lower bit rate is based on CELP and provides system designers with additional flexibility.

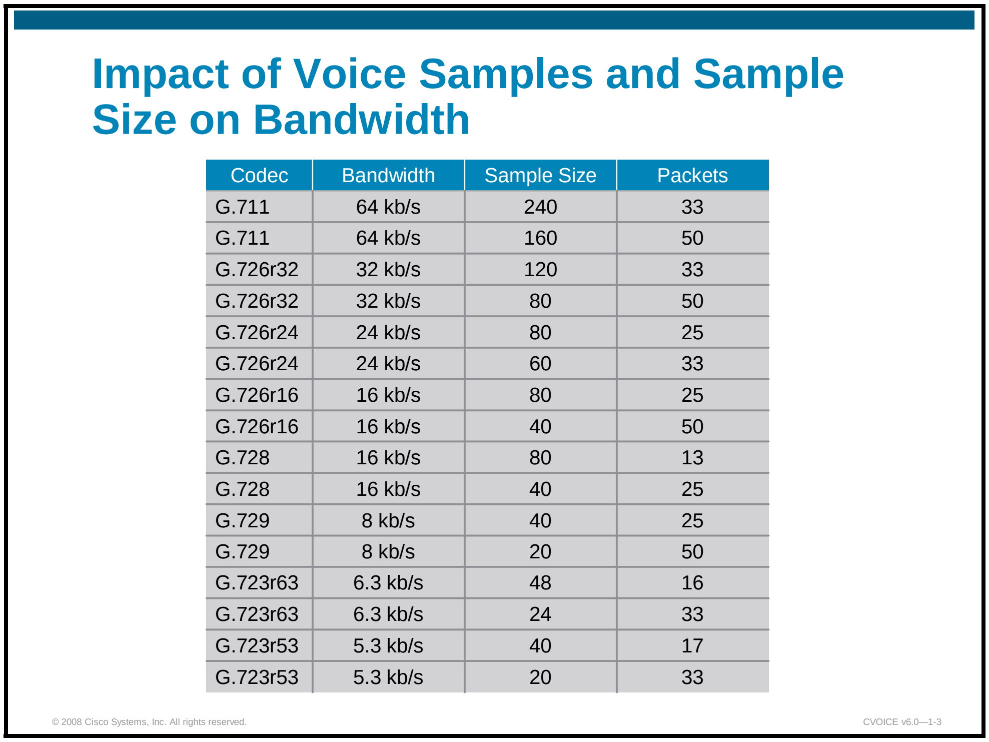
- **Global System for Mobile Communications Full Rate (GSM FR) codec:** Introduced in 1987, GSM FR has a frame size of 20 ms and operates at a bit rate of 13 kb/s. It is a Regular Pulse Excited-Linear Predictive (RPE-LTP) coder. In order to write Voice Extensible Markup Language (VoiceXML) scripts that can function as the user interface for a simple voice-mail system, the network must support GSM FR codecs. The network messaging must be capable of recording a voice message and depositing the message to an external server for later retrieval. This codec supports the Cisco infrastructure and application partner components required for service providers to deploy unified messaging applications.
- **Internet Low Bit Rate Codec (iLBC):** Was designed for narrowband speech and results in a payload bit rate of 13.33 kb/s for 30 ms frames and 15.20 kb/s for 20 ms frames. The algorithm is a version of block-independent linear predictive coding, with the choice of data frame lengths of 20 and 30 ms. The encoded blocks have to be encapsulated in a suitable protocol for transport like Real-Time Transport Protocol (RTP). This codec enables graceful speech quality degradation in the case of lost frames, which occurs in connection with lost or delayed IP packets.

Note iLBC is supported on the Cisco AS5350XM Universal Gateway and Cisco AS5400XM Series Universal Gateways with voice feature cards (VFCs) and IP-to-IP gateways with no transcoding and conferencing.

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

Impact of Voice Samples and Packet Size on Bandwidth

This topic describes how the number of voice samples that are encapsulated impacts bandwidth requirements.



Impact of Voice Samples and Sample Size on Bandwidth

Codec	Bandwidth	Sample Size	Packets
G.711	64 kb/s	240	33
G.711	64 kb/s	160	50
G.726r32	32 kb/s	120	33
G.726r32	32 kb/s	80	50
G.726r24	24 kb/s	80	25
G.726r24	24 kb/s	60	33
G.726r16	16 kb/s	80	25
G.726r16	16 kb/s	40	50
G.728	16 kb/s	80	13
G.728	16 kb/s	40	25
G.729	8 kb/s	40	25
G.729	8 kb/s	20	50
G.723r63	6.3 kb/s	48	16
G.723r63	6.3 kb/s	24	33
G.723r53	5.3 kb/s	40	17
G.723r53	5.3 kb/s	20	33

Voice sample size is a variable that can affect the total bandwidth used. A voice sample is defined as the digital output from a codec DSP that is encapsulated into a protocol data unit (PDU). Cisco uses DSPs that sample output based on digitization of 10 ms 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.

The table in the figure illustrates various codecs and sample sizes and the number of packets that are required for VoIP to transmit 1 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).

Encapsulated Bytes Calculation 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), as follows:

Bytes_per_Sample = (*Sample_Size* * *Codec_Bandwidth*) / 8

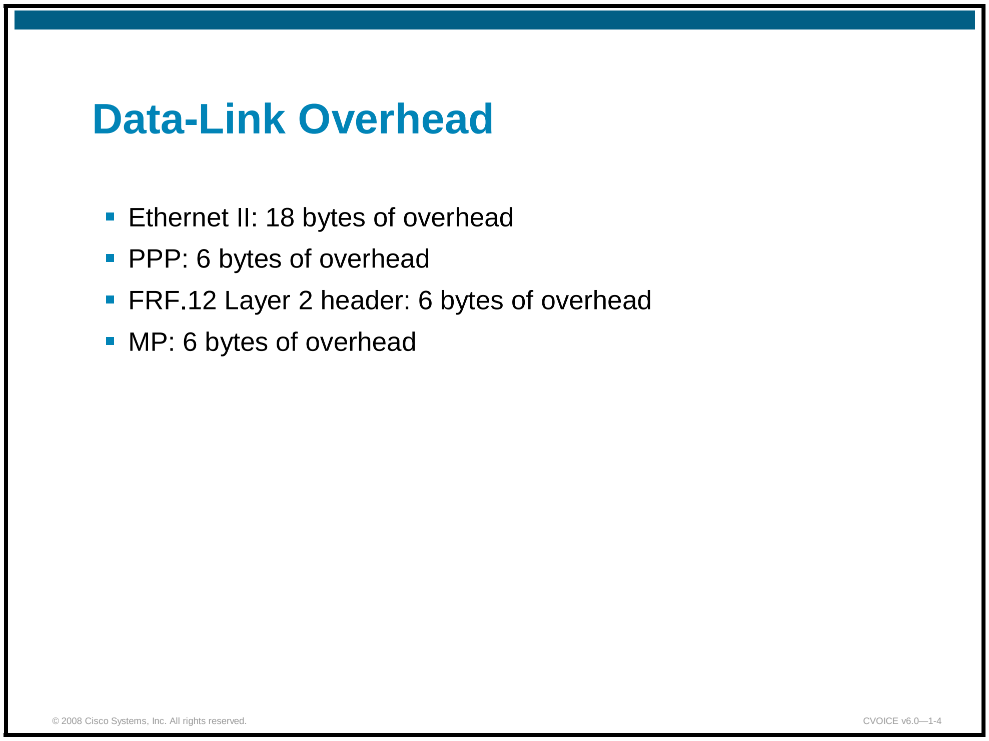
If you apply G.711 numbers, the formula reveals the following:

Bytes_per_Sample = (0.020 * 64,000) / 8

Bytes_per_Sample = 160

Calculating Overhead

This topic describes how to calculate the overhead for Layer 2 and other protocols on a VoIP call.



Data-Link Overhead

- Ethernet II: 18 bytes of overhead
- PPP: 6 bytes of overhead
- FRF.12 Layer 2 header: 6 bytes of overhead
- MP: 6 bytes of overhead

Several factors must be included in calculating the overhead of a VoIP call. Layer 2 and security protocols add to the packet size significantly.

Data-Link Overhead

Another contributing factor to bandwidth is the Layer 2 protocol that is used to transport VoIP. VoIP alone carries a 40-byte IP/User Datagram Protocol (UDP)/RTP header when that Layer 2 protocol is using uncompressed RTP. Depending on the Layer 2 protocol that is used, the overhead could grow substantially. The larger the Layer 2 overhead, the more bandwidth that is required to transport VoIP. These are 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).
- **PPP:** Carries 6 bytes of overhead; 1 flag byte to indicate the beginning or end of a frame, 1 address byte, 1 control byte, 1 protocol byte, and 2 bytes for CRC.
- **Frame Relay Fragmentation Implementation Agreement (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
- **Multilink PPP (MP):** Carries 6 bytes of overhead; 1 byte for flag, 1 byte for address, 2 bytes for control (or type), and 2 bytes for CRC.

IP Overhead

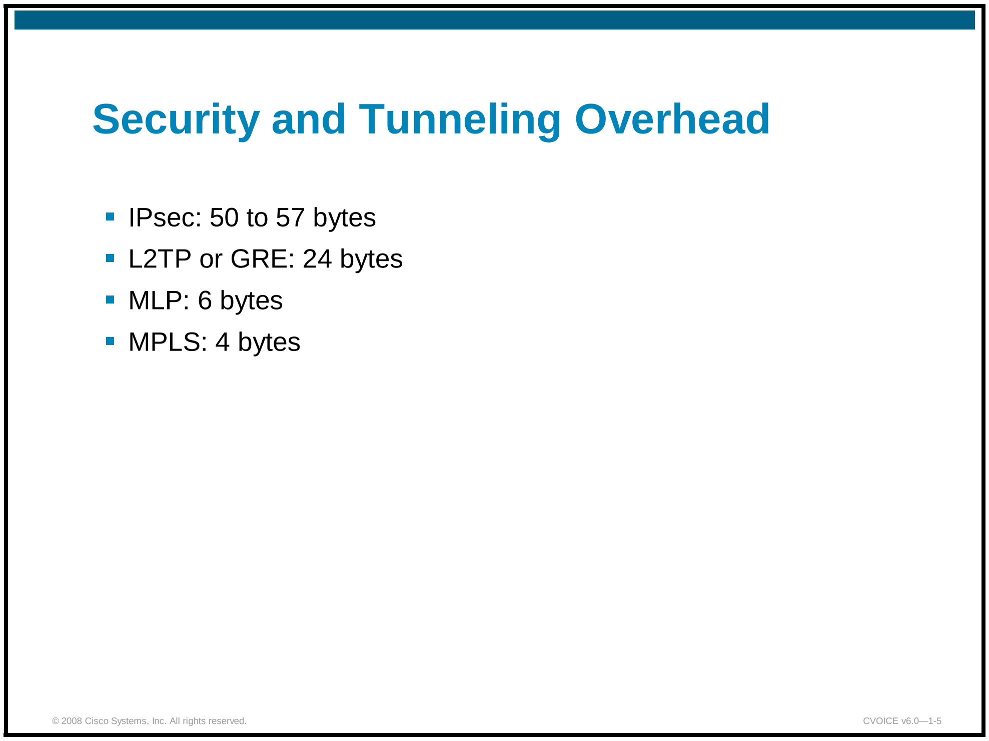
The IP and transport layers also have overhead to contribute to the size of the packets.

Here are some upper layer overhead.

- **IP:** Adds a 20 byte header..
- **UDP:** Adds an 8 byte header..
- **RTP:** Adds a 12 byte header.

Security and Tunneling Overhead

This subtopic covers security and tunneling overhead.



Security and Tunneling Overhead

- IPsec: 50 to 57 bytes
- L2TP or GRE: 24 bytes
- MLP: 6 bytes
- MPLS: 4 bytes

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-5

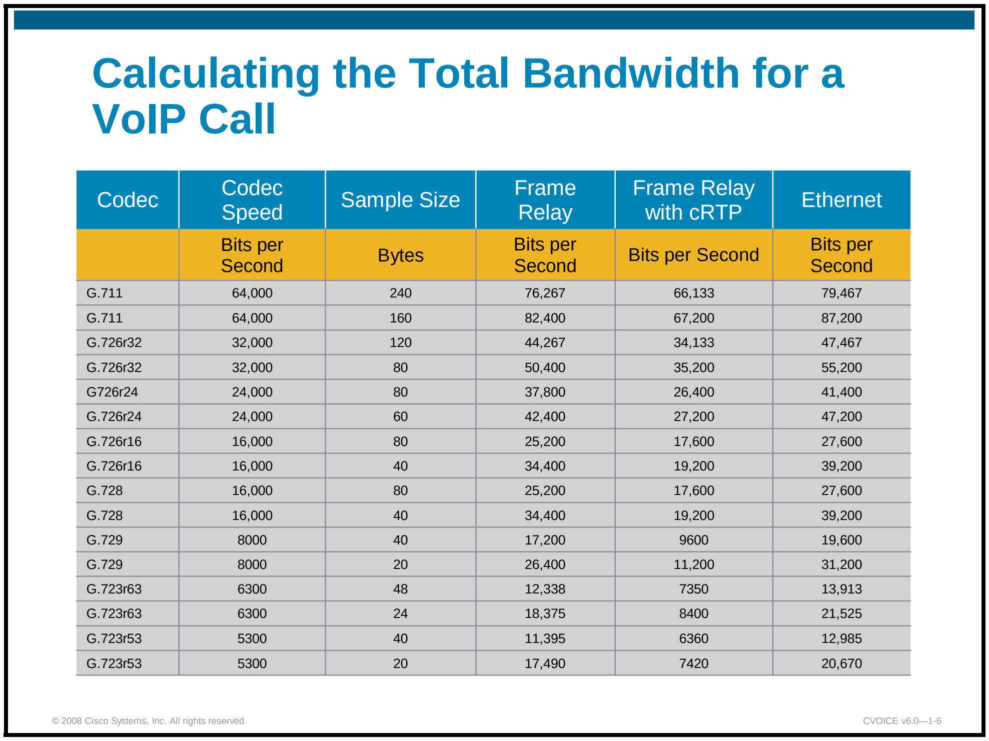
Certain security and tunneling encapsulations will also add overhead to voice packets and should be considered when calculating bandwidth requirements. When you are using a virtual private network (VPN), IP Security (IPsec) will add 50 to 57 bytes of overhead. This is a significant amount of overhead when considering small voice packets. Layer 2 Tunneling Protocol (L2TP) or Generic Routing Encapsulation (GRE) adds 24 bytes. When you are using MLP, 6 bytes will be added to each packet. Multiprotocol Label Switching (MPLS) adds a 4-byte label to every packet. All these specialized tunneling and security protocols must be considered when planning for bandwidth demands.

VPN Overhead Example

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

Calculating the Total Bandwidth for a VoIP Call

This topic describes how to calculate the total bandwidth that is required for a VoIP call with and without voice activity detection (VAD).



Calculating the Total Bandwidth for a VoIP Call

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

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

- If more bandwidth is required for the codec, then more total bandwidth is required.
- If more overhead is associated with the data link, then more total bandwidth is required.
- If there is a larger sample size, then less total bandwidth is required.
- If cRTP is being used, the total bandwidth that is required is significantly reduced.

Total Bandwidth Calculation Without VAD Example

As a network administrator, your task is to determine proper WAN link sizing to meet the requirements of the network. First, you will need to calculate the total bandwidth for each VoIP call. You may then use this information to calculate the total bandwidth required for the company WAN links.

Scenario

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

Use the following formula to calculate total bandwidth per call:

```
Total Bandwidth = total packet size x PPS
```

Where:

- Total packet size in bytes = (Layer 2 header: MP, FRF.12, or Ethernet) + (IP/UDP/RTP header) + (voice payload size)
- Total packet size in bits = total packet size in bytes x 8 bits per byte
- Packets Per Second (PPS) = codec bit rate / voice payload size
- Bandwidth = total packet size x PPS

These protocol header assumptions are used for the calculations that follow.

- 40 bytes for IP (20 bytes) / User Datagram Protocol (UDP) (8 bytes) / Real-Time Transport Protocol (RTP) (12 bytes) headers
- Compressed Real-Time Protocol (cRTP) reduces the IP/UDP/RTP headers to 2or 4bytes (cRTP is not available over Ethernet)
- 6 bytes for MP or FRF.12 Layer 2 (L2) header
- 1 byte for the end-of-frame flag on MP and Frame Relay frames
- 18 bytes for Ethernet L2 headers, including 4 bytes of Frame Check Sequence (FCS) or Cyclic Redundancy Check (CRC)

The calculation for the G.729 codec (8kb/s) with a 20-byte sample size and using FRF.12 *without* cRTP is as follows:

- Total packet size (bytes) = 6 bytes (FRF.12) + 40 bytes (IP/UDP/RTP) + 20 bytes (payload) = 66 bytes
- Total packet size (bits) = 66 bytes * 8 bits per byte = 528 bits
- PPS = 8 kb/s / 160 bits = 50 p/s

Note 160 bits = 20 bytes (default voice payload) * 8 bits per byte.

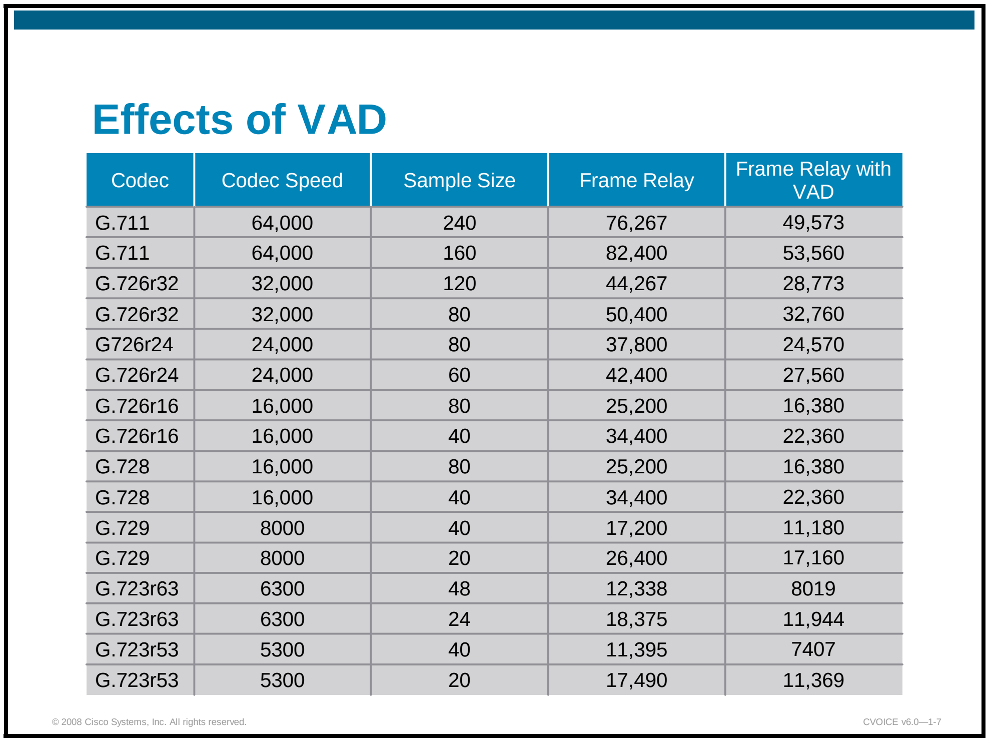
- Bandwidth per call = 528 bits/p * 50 p/s = 26400b/s = 26.4 kb/s

The calculation for the G.729 codec, 20-byte sample size, using FRF.12 *with* cRTP is as follows:

- Total packet size in bytes = 6 bytes + 2 bytes + 20 bytes = 28 bytes
- Total packet size (bits) = 28 bytes * 8 bits per byte = 224 bits
- PPS = 8 kb/s / 160 bits = 50 p/s
- Bandwidth per call = 224 bits/p * 50 p/s = 11200b/s = 11.2 kb/s

Effects of VAD on Bandwidth

This subtopic describes the effect of VAD on total bandwidth.



Effects of VAD

Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with VAD
G.711	64,000	240	76,267	49,573
G.711	64,000	160	82,400	53,560
G.726r32	32,000	120	44,267	28,773
G.726r32	32,000	80	50,400	32,760
G726r24	24,000	80	37,800	24,570
G.726r24	24,000	60	42,400	27,560
G.726r16	16,000	80	25,200	16,380
G.726r16	16,000	40	34,400	22,360
G.728	16,000	80	25,200	16,380
G.728	16,000	40	34,400	22,360
G.729	8000	40	17,200	11,180
G.729	8000	20	26,400	17,160
G.723r63	6300	48	12,338	8019
G.723r63	6300	24	18,375	11,944
G.723r53	5300	40	11,395	7407
G.723r53	5300	20	17,490	11,369

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

VAD provides a maximum of 35 percent bandwidth savings based on an average volume of more than 24 calls. Bandwidth savings of 35 percent is a subjective figure and does not take into account loud background sounds, differences in languages, and other factors.

The savings will vary on every individual voice call or on any specific point measurement.

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

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

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

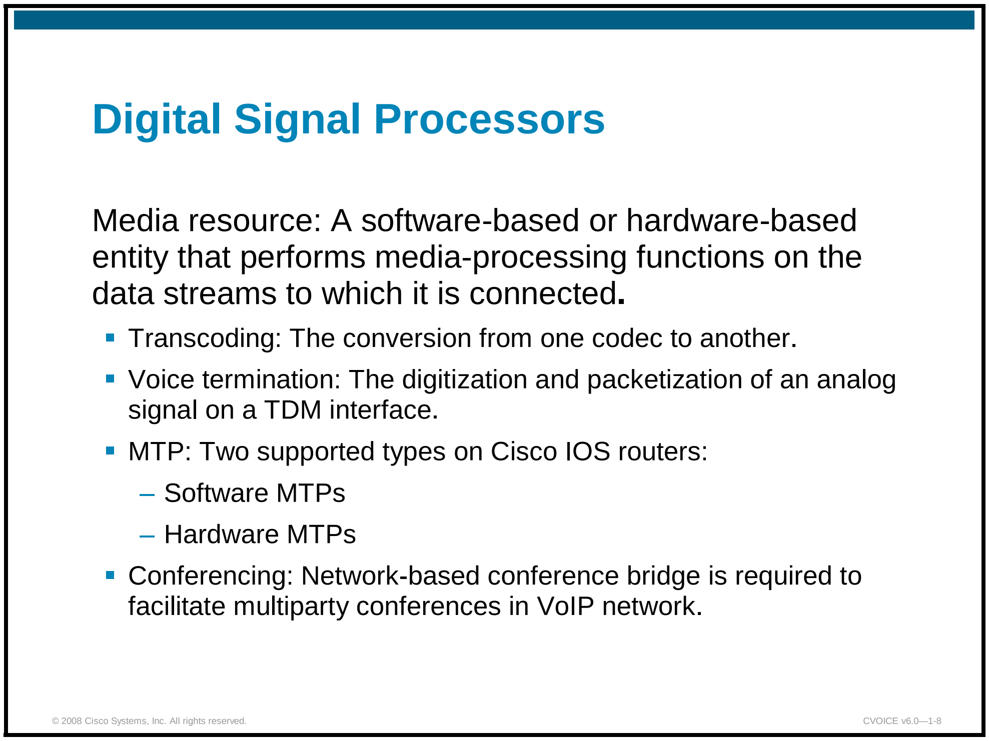
VAD Bandwidth Savings Example

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

Caution Voice quality may vary widely when VAD is used.

Digital Signal Processors

This topic describes various types of DSPs, DSP functions, and how DSPs are used as media resources.



Digital Signal Processors

Media resource: A software-based or hardware-based entity that performs media-processing functions on the data streams to which it is connected**.**

- Transcoding: The conversion from one codec to another.
- Voice termination: The digitization and packetization of an analog signal on a TDM interface.
- MTP: Two supported types on Cisco IOS routers:
  - Software MTPs
  - Hardware MTPs
- Conferencing: Network-based conference bridge is required to facilitate multiparty conferences in VoIP network.

CVOICE v6.0—1-8

A DSP is a specialized microprocessor designed specifically for digital signal processing. DSPs enable Cisco platforms to efficiently process digital voice traffic. DSPs on a router provide stream-to-packet signal processing functionality that includes voice compression, echo cancellation, and tone- and voice-activity detection.

A media resource is a software-based or hardware-based entity that performs media-processing functions on the data streams to which it is connected. Media-processing functions include mixing multiple streams to create one output stream (conferencing), passing the stream from one connection to another (Media Termination Point [MTP]), converting the data stream from one compression type to another (transcoding), echo cancellation, signaling, termination of a voice stream from a time-division multiplexing (TDM) circuit (coding/decoding), packetization of a stream, streaming audio (annunciation), and so forth.

The terms “DSP” and “media resource” are often used interchangeably in some documentation.

The four major functions of DSPs in a voice gateway are as follows:

- **Transcoding:** The direct digital-to-digital conversion from one (usually lossy) codec to another. Transcoding compresses and decompresses voice streams to match endpoint-device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth, but the local device does not support that type of compression. Ideally, all IP telephony devices would support the same codecs, but this is not the case. Rather, different devices support different codecs.

Transcoding is processed by DSPs on the DSP farm; sessions are initiated and managed by Cisco Unified Communications Manager. Cisco Unified Communications Manager also refers to transcoders as hardware MTPs.

If an application or service can handle only one specific codec type, which is usually G.711, a G.729 call from a remote site must be transcoded to G.711. This can only be done via DSP resources. Because applications and services are often hosted in main sites, DSP transcoding resources are most common in central sites.

- **Voice termination:** Applies to a call that has two call legs, one leg on a TDM interface and the second leg on a VoIP connection. The TDM leg must be terminated by hardware that performs coding/decoding and packetization of the stream. DSPs perform this termination function. The DSP also provides echo cancellation, VAD, and jitter management at the same time it performs voice termination.
- **Audio conferencing:** In a traditional circuit-switched voice network, all voice traffic goes through a central device (such as a PBX system), which provides audio conferencing services as well. Because IP phones transmit voice traffic directly between phones, a network-based conference bridge is required to facilitate multiparty conferences.

  A conference bridge is a resource that joins multiple participants into a single call. It can accept any number of connections for a given conference, up to the maximum number of streams allowed for a single conference on that device. There is a one-to-one correspondence between media streams that are connected to a conference and participants that are connected to the conference. The conference bridge mixes the streams together and creates a unique output stream for each connected party. The output stream for a given party is the composite of the streams from all connected parties minus their own input stream. Some conference bridges mix only the three loudest talkers on the conference and distribute that composite stream to each participant (minus their own input stream if they are one of the talkers).

  Hardware conference bridges are used in two environments. They can be used to increase the conferencing capacity in a central site without putting an additional load on Cisco Unified Communications Manager servers, which can host software-based conference bridges. More important, hardware conference bridges are also used in remote sites. If no remote-site conference resources are deployed, every conference will be routed to central resources, resulting in sometimes excessive WAN usage.

  In addition, DSP-based conference bridges can mix G.711 and G.729 calls, thus supporting any call-type scenario in multisite environments. In contrast, software-based conference bridges deployed on Cisco Unified Communications Manager servers can mix only G.711 calls.
- **MTP:** An entity that accepts two full-duplex voice streams using the same codec. It bridges the media streams together and allows them to be set up and torn down independently. The streaming data that is received from the input stream on one connection is passed to the output stream on the other connection, and vice versa. In addition, the MTP can be used to transcode a-law to mu-law and vice versa, or it can be used to bridge two connections that utilize different packetization periods (different packet sizes). MTPs are also used to provide further processing of a call, such as RFC 2833 support.

MTPs have many possible uses, as described in the following sections.

Repacketization

An MTP can be used to transcode a-law to mu-law and vice versa, or it can be used to bridge two connections that utilize different packetization periods (different sample sizes).

H.323 Supplementary Services

MTPs can be used to extend supplementary services to H.323 endpoints that do not support the H.323v2 OpenLogicalChannel and CloseLogicalChannel request features of the Empty Capability Set (ECS). This requirement occurs infrequently. Cisco H.323 endpoints support ECS, and most third-party endpoints have support as well. When needed, an MTP is allocated and connected into a call on behalf of an H.323 endpoint. Once inserted, the media streams are connected between the MTP and the H.323 device, and these connections are present for the duration of the call. The media streams connected to the other side of the MTP can be connected and disconnected as needed to implement features such as hold, transfer, and so forth.

When an MTP is required on an H.323 call and there is not one available, the call will proceed but will not be able to invoke supplementary services.

Note Implementations prior to Cisco Unified Communications Manager Release 3.2 required MTPs to provide supplementary services for H.323 endpoints, but Cisco Unified Communications Manager Release 3.2 and later no longer require MTP resources to provide this functionality.

MTP Types

There are two types of MTPs that are supported on Cisco IOS routers:

- **Software MTP:** A resource that you can implement by installing the Cisco IP Voice Media Streaming Application on a Cisco Unified Communications Manager server or by using a Cisco IOS gateway without using DSP resources. A software MTP device supports G.711 to G.711 and G.729 to G.729 streams. A Cisco IOS software-enhanced device may be implemented on a Cisco IOS router by configuring a software-only MTP under a DSP farm. This DSP farm may be used only as a pure MTP and does not require any hardware DSPs on the router. These are examples of the two types of software MTPs:
  - Cisco IP Voice Media Streaming Application
    - This software MTP is a device that is implemented by installing the Cisco IP Voice Media Streaming Application on a server. When the installed application is configured as an MTP application, it registers with a Cisco Unified Communications Manager node and informs Cisco Unified Communications Manager of how many MTP resources it supports. A software MTP device supports only G.711 streams. The Cisco IP Voice Media Streaming Application is a resource that may also be used for several functions, and proper design must consider all functions together.
  - Cisco IOS software-based
    - This MTP allows configuration of any of the following codecs, but only one may be configured at a given time: G.711 mu-law and a-law, G.729A, G.729, G.729 Annex A with Annex B (G.729AB), G.729 Annex B (G.729B), GSM, and pass-through. Some of these are not pertinent to a Cisco Unified Communications Manager implementation.

    - The router configuration permits up to 500 individual streams, which support 250 transcoded sessions. This number of G.711 streams generates 5 Mbytes of traffic.

- **Hardware MTP:** A resource that uses gateway-based DSPs to interconnect two G.711 streams. This connection is made without the use of the gateway CPU. This hardware-only implementation uses a DSP resource for endpoints that use the same G.711 codec but a different packetization time. The repacketization requires a DSP resource so it cannot be done by software only. Examples include the following:

  — Cisco NM-HDV2, NM-HD-1V, NM-HD-2V, and NM-HD-2VE, and Cisco 2800 and 3800 Series Integrated Services Routers:

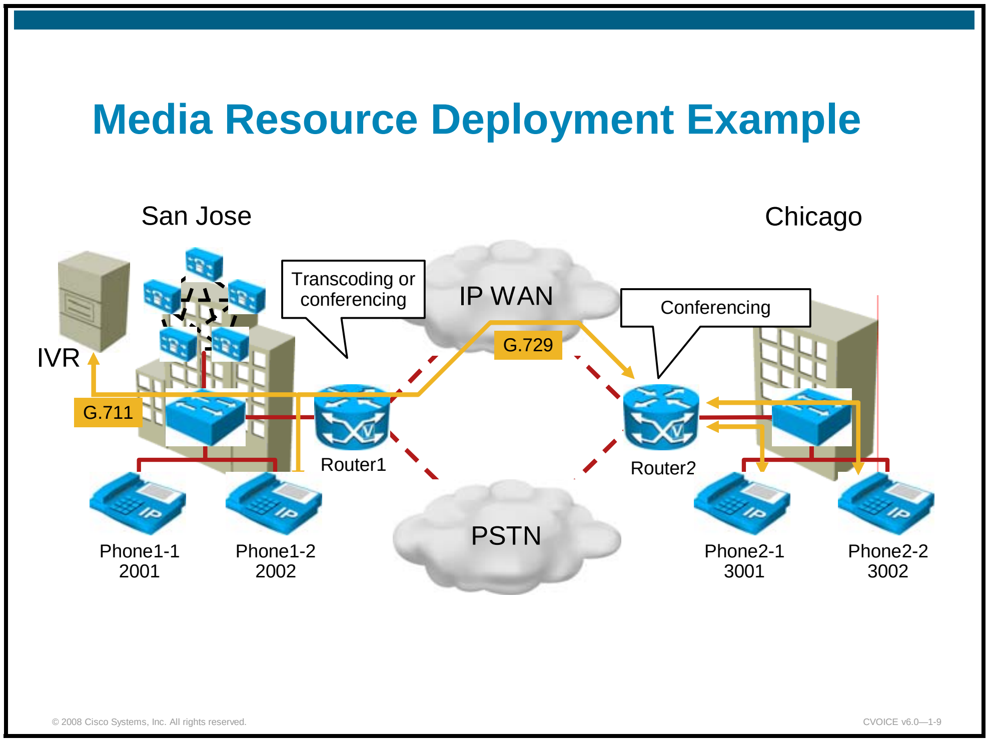
    - These hardware products use the packet voice DSP module, generation 2 (PVDM-2) modules for providing DSPs.
    - Each DSP can provide 16 G.711 mu-law or a-law MTP sessions or 6 G.729, G.729B, or GSM MTP sessions.

  — Cisco WS-SVC-CMM-ACT Communication Media Module:

    - This module has four DSPs that may be configured individually.
    - Each DSP can support 128 G.729, G.729B, or GSM MTP sessions or 256 G.711 mu-law or a-law MTP sessions.

  — Catalyst WS-X6608-T1 and WS-X6608-E1 Digital Gateway Cards for the Cisco Catalyst 6000 platform switches:

    - Codec support is G.711 mu-law or a-law, G.729, G.720B, or GSM.
    - Configuration is done at the port level. Eight ports are available per module.
    - Each port configured as an MTP resource provides 24 sessions.



Media Resource Deployment Example

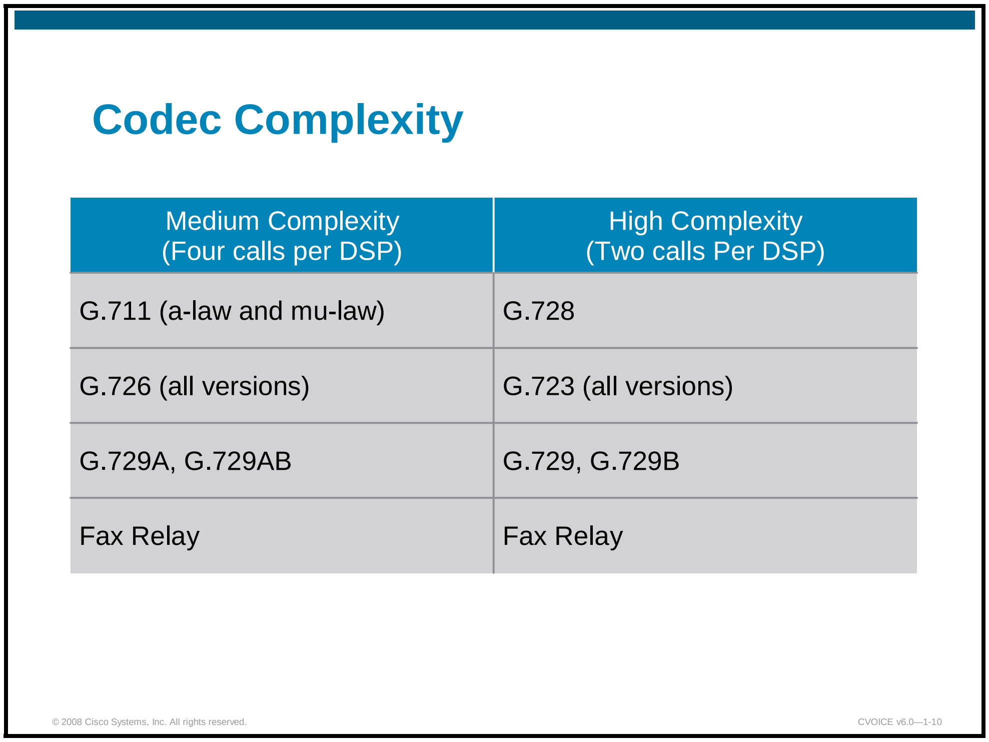
CVOICE v6.0—1-9

The figure shows a multisite environment with deployed DSP resources. Router2 in Chicago is offering DSP-based conferencing services to support mixed codec environments and optimal WAN usage.

The central gateway Router1 offers transcoding and conferencing services. The transcoding resources can be used to transcode G.729 to G.711 and then connect to an application server or even a software-based Cisco Unified Communications Manager conference bridge.

Codec Complexity

This topic describes codec complexity and where and how to configure it.



Codec Complexity

Medium Complexity (Four calls per DSP)	High Complexity (Two calls Per DSP)
G.711 (a-law and mu-law)	G.728
G.726 (all versions)	G.723 (all versions)
G.729A, G.729AB	G.729, G.729B
Fax Relay	Fax Relay

CVOICE v6.0—1-10

Codec complexity refers to the amount of processing that is required to perform voice compression. Codec complexity affects call density, which is the number of calls that are reconciled on the DSPs. With higher codec complexity, fewer calls can be handled. Select a higher codec complexity when high complexity is required to support a particular codec or combination of codecs. Select a lower codec complexity to support the greatest number of voice channels, provided that the lower complexity is compatible with the particular codecs in use.

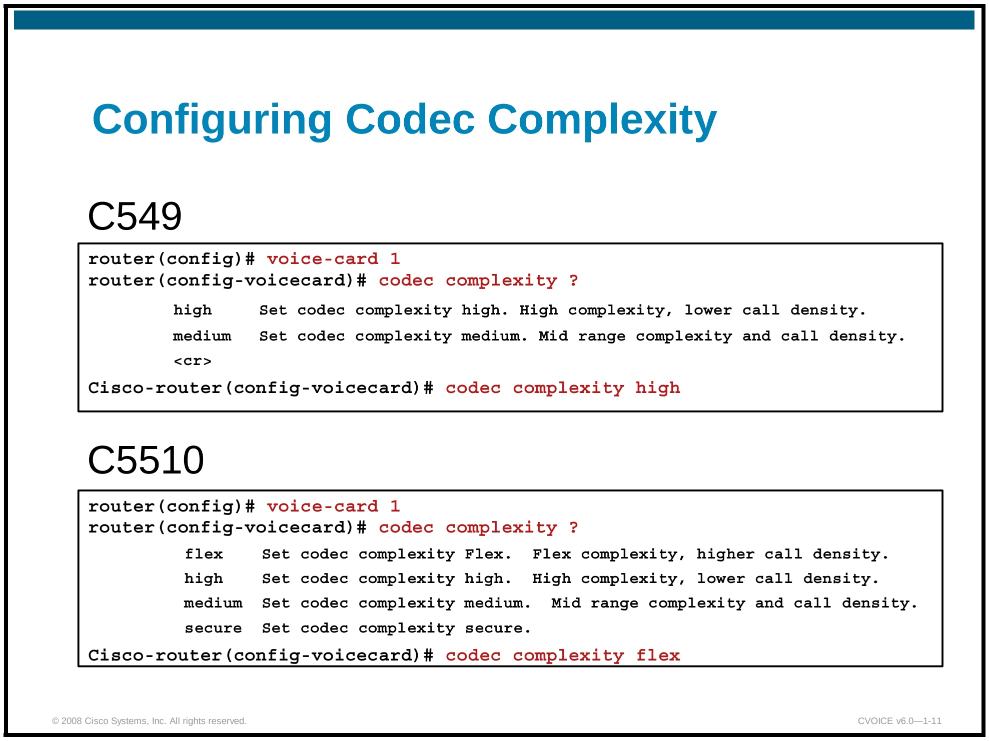
Some codec compression techniques require more processing power than others. Codec complexity is broken into two categories named medium and high complexity.

- Medium complexity allows the C549 DSPs to process up to four voice or fax relay calls per DSP and the C5510 DSPs to process up to eight voice or fax relay calls per DSP.
- High complexity allows the C549 DSPs to process up to two voice or fax relay calls per DSP and the C5510 DSPs to process up to six voice fax relay calls per DSP.

The difference between medium- and high-complexity codecs is the amount of CPU utilization necessary to process the codec algorithm, and therefore, the number of voice channels that can be supported by a single DSP. For this reason, all medium-complexity codecs can also be run in high-complexity mode, but fewer (usually about half) of the channels are available per DSP.

Configuring Codec Complexity

This subtopic describes how to configure codec complexity on platforms that support the C549 and C5510 DSP technologies.



Configuring Codec Complexity

C549

```
router(config)# voice-card 1
router(config-voicecard)# codec complexity ?
        high     Set codec complexity high. High complexity, lower call density.
        medium   Set codec complexity medium. Mid range complexity and call density.
        <cr>
Cisco-router(config-voicecard)# codec complexity high
```

C5510

```
router(config)# voice-card 1
router(config-voicecard)# codec complexity ?
         flex    Set codec complexity Flex.  Flex complexity, higher call density.
         high    Set codec complexity high.  High complexity, lower call density.
         medium  Set codec complexity medium.  Mid range complexity and call density.
         secure  Set codec complexity secure.
Cisco-router(config-voicecard)# codec complexity flex
```

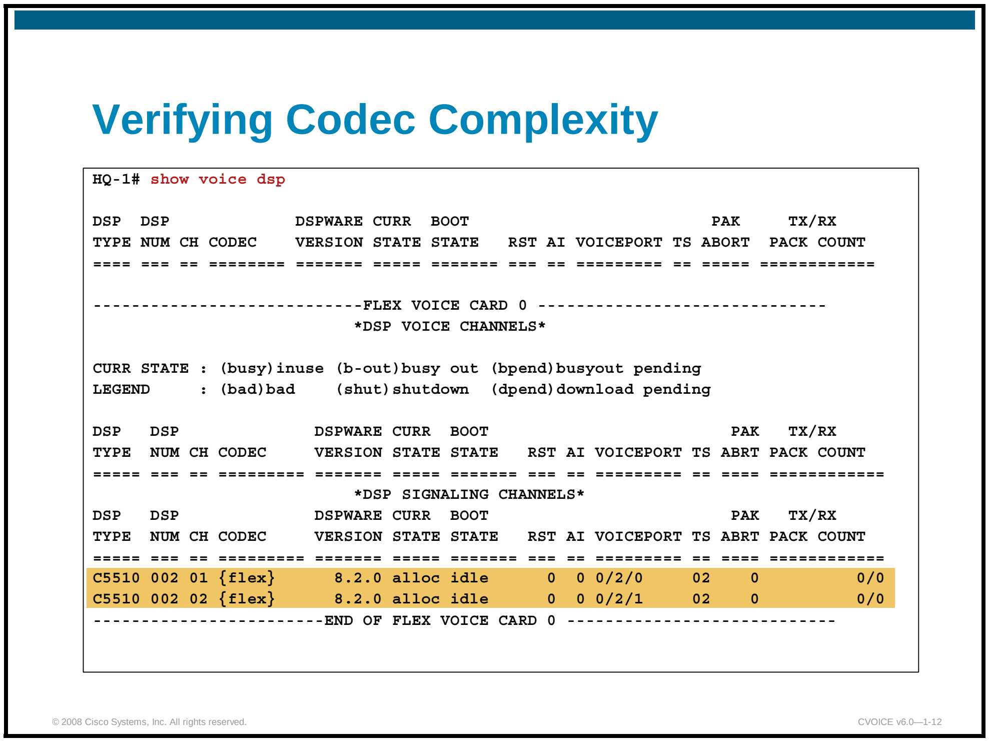
© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-11

On platforms that support the C549 DSP technology, the codec complexity is configured on the voice card (for example, the Cisco 2600 Series and 3600 Multiservice Platforms and the Cisco Voice Gateway 200 Series Gateways [VG200] NM-HDV). Some platforms support only high complexity because they have enough DSPs onboard to support all T1/E1 channels that use the high complexity mode. To specify call density and codec complexity according to the codec standard that is used, use the **codec complexity** command in voice card configuration mode.

On platforms that support C5510 DSP technology, an additional option of flex complexity is available. When you use flex complexity, up to 16 calls can be completed per DSP. The number of supported calls varies from 6 to 16 and is based on the codec that is used for a call.

Verifying Codec Complexity

This subtopic describes how to verify codec complexity on a router.



Verifying Codec Complexity

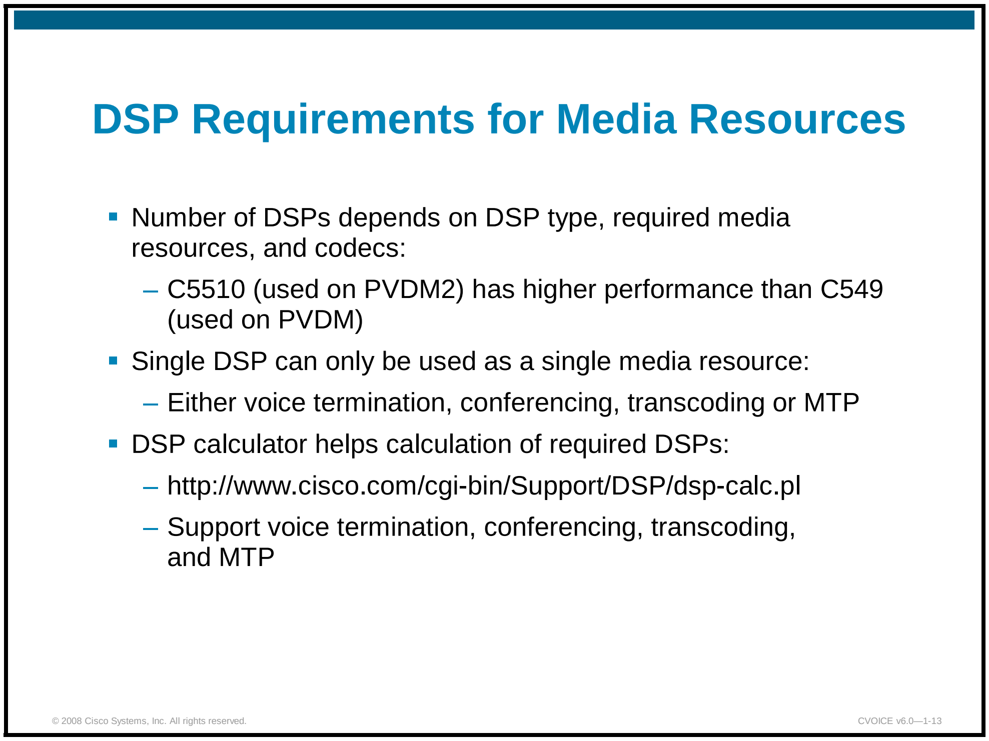
```
HQ-1# show voice dsp

DSP  DSP             DSPWARE CURR  BOOT                         PAK     TX/RX
TYPE NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABORT  PACK COUNT
==== === == ======== ======= ===== ======= === == ========= == ===== ============

----------------------------FLEX VOICE CARD 0 ------------------------------
                           *DSP VOICE CHANNELS*

CURR STATE : (busy)inuse (b-out)busy out (bpend)busyout pending
LEGEND     : (bad)bad    (shut)shutdown  (dpend)download pending

DSP   DSP              DSPWARE CURR  BOOT                         PAK   TX/RX
TYPE  NUM CH CODEC     VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ========= ======= ===== ======= === == ========= == ==== ============
                           *DSP SIGNALING CHANNELS*
DSP   DSP              DSPWARE CURR  BOOT                         PAK   TX/RX
TYPE  NUM CH CODEC     VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ========= ======= ===== ======= === == ========= == ==== ============
C5510 002 01 {flex}      8.2.0 alloc idle      0  0 0/2/0     02    0          0/0
C5510 002 02 {flex}      8.2.0 alloc idle      0  0 0/2/1     02    0          0/0
------------------------END OF FLEX VOICE CARD 0 ----------------------------
```

CVOICE v6.0—1-12

Use the **show voice dsp** command to verify codec complexity configurations.

DSP Requirements for Media Resources

This topic describes the DSP requirements for various media resources and shows how to calculate the actual number of required DSPs.



DSP Requirements for Media Resources

- Number of DSPs depends on DSP type, required media resources, and codecs:
  - C5510 (used on PVDM2) has higher performance than C549 (used on PVDM)
- Single DSP can only be used as a single media resource:
  - Either voice termination, conferencing, transcoding or MTP
- DSP calculator helps calculation of required DSPs:
  - http://www.cisco.com/cgi-bin/Support/DSP/dsp-calc.pl
  - Support voice termination, conferencing, transcoding, and MTP

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-13

The number of required DSPs is a key factor when you are deploying media resources that use DSPs. This mainly depends on two factors: DSP type and the codec being used. In general, the old packet voice/data modules (PVDMs) support less sessions than the new packet voice DSP module, generation 2 (PVDM2), and G.711-only media resources require less resources than mixed-codec or G.729 resources.

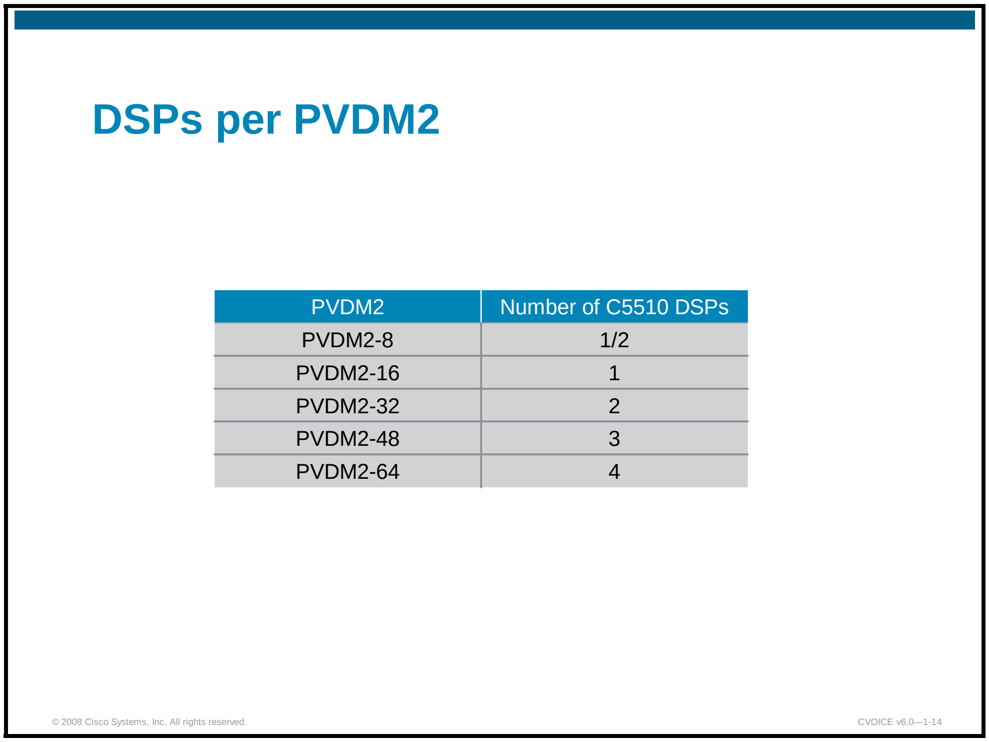
Resource Allocation on the NM-HDV (C549-Based Hardware)

You configure each DSP individually, and each DSP functions independently of the others. The conferencing and transcoding MTP resources must be allocated to different DSPs, and a single DSP can support only one of these functions at a time. The configuration specifies which function each DSP will perform.

An NM-HDV may be associated with only a single Cisco Unified Communications Manager.

Resource Allocation on the NM-HDV2, NM-HD-xx, and PVDM2 (C5510-Based Hardware)

Hardware resources based on the C5510 chipset are allocated using DSP profiles that define the resource type within the profile. Multiple profiles can be defined on a single gateway. These profiles may then be registered to different Cisco Unified Communications Manager clusters.

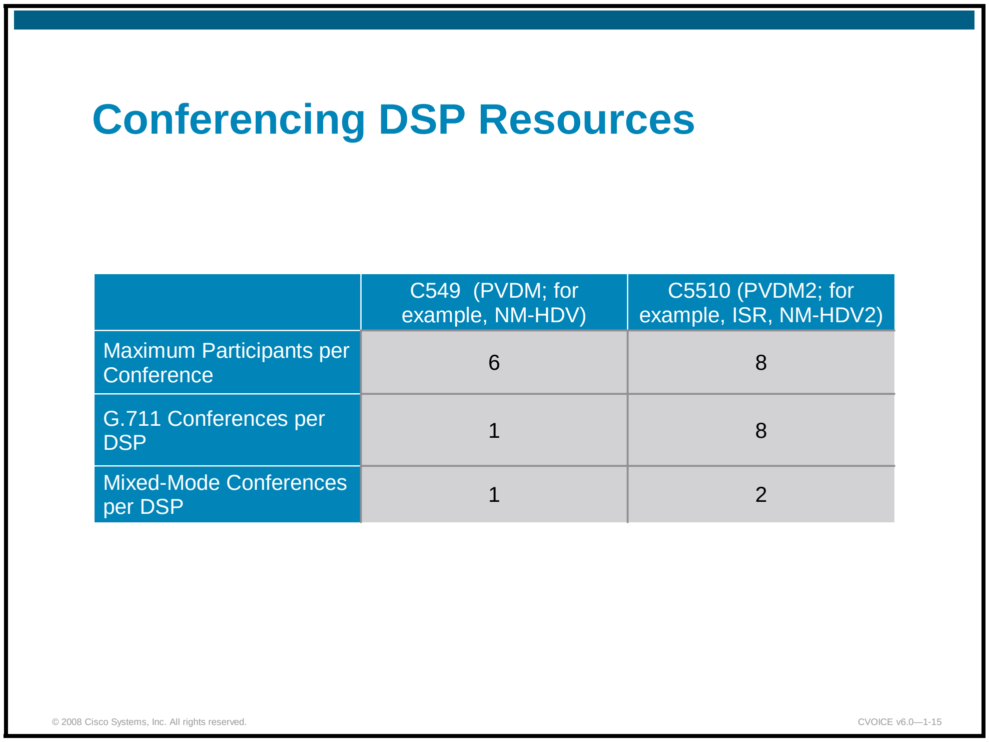


DSPs per PVDM2

PVDM2	Number of C5510 DSPs
PVDM2-8	1/2
PVDM2-16	1
PVDM2-32	2
PVDM2-48	3
PVDM2-64	4

A PVDM2 is a module that can carry up to four C5510 DSPs. The table in the figure lists the DSP per PVDM2 allocation.

Note Both the PVDM2-8 and the PVDM2-16 have a single DSP. The DSP on the PVDM2-8 has one-half the capacity of the DSP used on other PVDM2 modules. A PVDM2-8 can be used for conferencing but with lower performance numbers than the other DSPs.



Conferencing DSP Resources

	C549 (PVDM; for example, NM-HDV)	C5510 (PVDM2; for example, ISR, NM-HDV2)
Maximum Participants per Conference	6	8
G.711 Conferences per DSP	1	8
Mixed-Mode Conferences per DSP	1	2

CVOICE v6.0—1-15

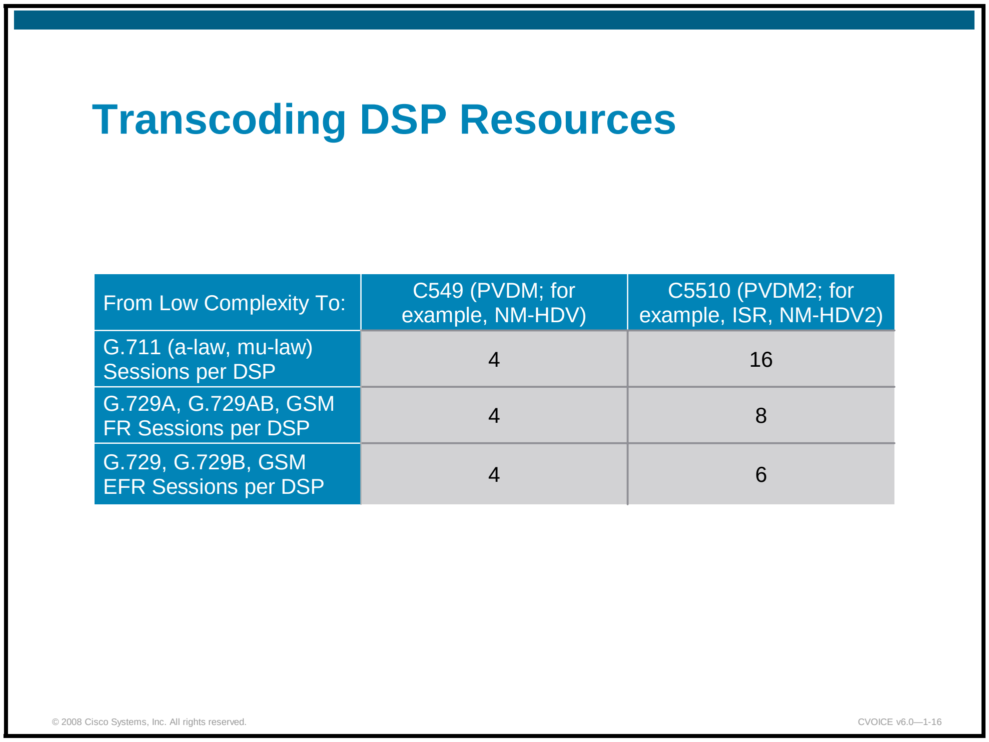
Conferencing resources can either be G.711-only or mixed mode, that is, at least one party has G.729. Mixed-mode conferences require more DSP resources because the DSP will perform transcoding and mixing operations.

Note For PVDM- and PVDM2-based conferencing, the maximum number of conference participants is independent from the maximum number of conferences. This means that whether a conference has three, five, or eight participants, it counts against the number of simultaneous conferences that are supported on a DSP.

The “Conferencing DSP Resources” table shows the various DSP resources for conferencing and their performance. As the table shows, the C5510 on the PVDM2, Integrated Services Router (ISR), and NM-HDV2 can handle more conferences and participants per conference.

Conferencing DSP Resources

Hardware Module or Chassis	DSP Configuration	Conferences	
		All Participants Use G.711 (a-law, mu-law)	One or More Participants Use G.729 or G.729A
NM-HDV2 (8 participants per conference)	1 to 4 of: PVDM2-8 (½ DSP) PVDM2-16 (1 DSP) PVDM2-32 (2 DSPs) PVDM2-48 (3 DSPs) PVDM2-64 (4 DSPs)	Conferences per PVDM2: 4 8 16 24 32 Maximum of 50 conferences per network module	Conferences per PVDM2: 1 2 4 6 8
NM-HD-1V (8 participants per conference)	Fixed at 1 DSP	8 conferences per network module	2 conferences per network module
NM-HD-2V (8 participants per conference)	Fixed at 1 DSP	8 conferences per network module	2 conferences per network module
NM-HD-2VE (8 participants per conference)	Fixed at 3 DSPs	24 conferences per network module	6 conferences per network module
NM-HDV NM-HDV-FARM (6 participants per conference)	1 to 5 of PVDM-12 (3 DSPs per PVDM-12)	3, 6, 9, 12, or 15 conferences per network module	3, 6, 9, 12, or 15 conferences per network module
Cisco 1751 Modular Access Router (6 participants per conference)	1 to 2 of: PVDM-256K-4 (1 DSP) PVDM-256K-8 (2 DSPs) PVDM-256K-12 (3 DSPs) PVDM-256K-16HD (4 DSPs) PVDM-256K-20HD (5 DSPs)	1 conference per DSP Maximum of 5 conferences per chassis	1 conference per DSP Maximum of 5 conferences per chassis
Cisco 1760 Modular Access Router (6 participants per conference)	1 to 2 of: PVDM-256K-4 (1 DSP) PVDM-256K-8 (2 DSPs) PVDM-256K-12 (3 DSPs) PVDM-256K-16HD (4 DSPs) PVDM-256K-20HD (5 DSPs)	1 conference per DSP Maximum of 20 conferences per chassis	1 conference per DSP Maximum of 20 conferences per chassis
Catalyst 6000 WS-6608-T1 and WS-6608-E1 (3 to 32 participants per conference)	Fixed at 64 of C549 (8 DSPs per port)	32 participants per port	32 participants per port G.729A and G.711 only
WS-SVC-CMM-ACT Communication Media Module (64 participants per conference)	Fixed at 4 of Broadcom 1500	128 conferences per module	128 conferences per module



Transcoding DSP Resources

From Low Complexity To:	C549 (PVDM; for example, NM-HDV)	C5510 (PVDM2; for example, ISR, NM-HDV2)
G.711 (a-law, mu-law) Sessions per DSP	4	16
G.729A, G.729AB, GSM FR Sessions per DSP	4	8
G.729, G.729B, GSM EFR Sessions per DSP	4	6

CVOICE v6.0—1-16

The number of required DSPs for transcoding depends on the DSP type that is used and the codecs that need to be transcoded. C549 supports up to four transcoding sessions for any codec combination. The C5510 supports 16 G.711 sessions; 8 G.729A, G.729AB, and GSM FR sessions; and 6 G729, G729B, and GSM-E FR sessions.

The “Transcoding DSP Resources” table shows the various DSP resources that can be used for transcoding and their performance.

Transcoding DSP Resources

Hardware Module or Chassis	DSP Configuration	Conferences	
		All Participants Use G.711 (a-law, mu-law)	**One or More Participants Use G.729 or G.729A**
NM-HDV2	1 to 4 of: ■ PVDM2-8 (½ DSP) ■ PVDM2-16 (1 DSP) ■ PVDM2-32 (2 DSPs) ■ PVDM2-48 (3 DSPs) ■ PVDM2-64 (4 DSPs)	Sessions per PVDM2 8 16 32 48 64	Sessions per PVDM2 4 8 16 24 32
NM-HD-1V	Fixed at 1 DSP	16 sessions per network module	8 sessions per network module
NM-HD-2V	Fixed at 1 DSP	16 sessions per network module	8 sessions per network module

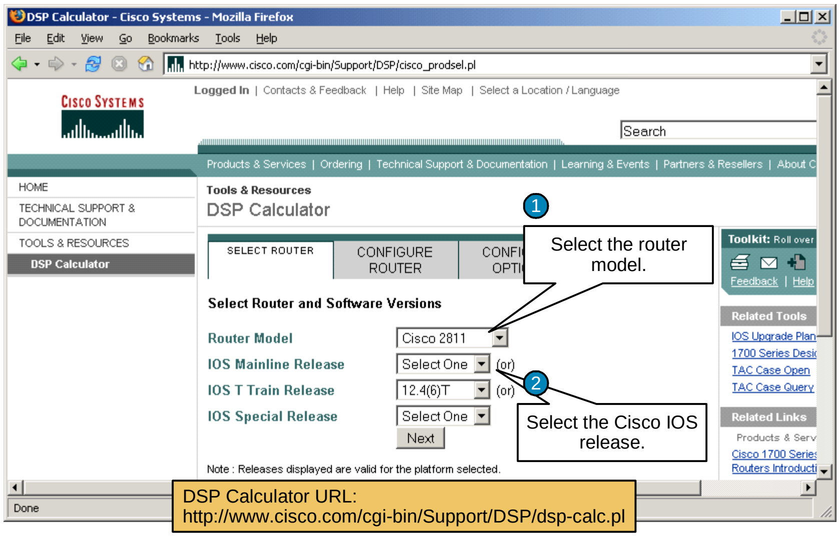
Hardware Module or Chassis	DSP Configuration	Conferences	
		All Participants Use G.711 (a-law, mu-law)	One or More Participants Use G.729 or G.729A
NM-HD-2VE	Fixed at 3 DSPs	48 sessions per network module	24 sessions per network module
NM-HDV NM-HDV-FARM	1 to 5 of PVDM-12 (3 DSPs per PVDM-12)	12, 24, 36, 48, or 60 sessions per network module	12, 24, 36, 48, or 60 sessions per network module
1751 Modular Access Router	1 to 2 of: ■ PVDM-256K-4 (1 DSP) ■ PVDM-256K-8 (2 DSPs) ■ PVDM-256K-12 (3 DSPs) ■ PVDM-256K-16HD (4 DSPs) ■ PVDM-256K-20HD (5 DSPs)	2 sessions per DSP Maximum of 16 sessions per chassis	2 sessions per DSP Maximum of 16 sessions per chassis
1760 Modular Access Router	1 to 2 of: ■ PVDM-256K-4 (1 DSP) ■ PVDM-256K-8 (2 DSPs) ■ PVDM-256K-12 (3 DSPs) ■ PVDM-256K-16HD (4 DSPs) ■ PVDM-256K-20HD (5 DSPs)	2 sessions per DSP Maximum of 20 sessions per chassis	2 sessions per DSP Maximum of 20 sessions per chassis
Catalyst 6000 WS-6608-T1 and WS-6608-E1	Fixed at 64 of C549 (8 DSPs per port)	24 sessions per port	24 sessions per port
WS-SVC-CMM-ACT	Fixed at 4 of Broadcom 1500	128 sessions per module	128 sessions per module

In addition to transcoding, DSPs can also be used as hardware MTPs. The “MTP DSP Resources for Enhanced Cisco IOS Media Resources” table shows the various DSPs that can be used as MTPs and their performance.

MTP DSP Resources for Enhanced Cisco IOS Media Resources

Hardware Module or Chassis	DSP Configuration	MTP G.711 (a-law, mu-law)
NM-HDV2	1 to 4 of: ■ PVDM2-8 (½ DSP) ■ PVDM2-16 (1 DSP) ■ PVDM2-32 (2 DSPs) ■ PVDM2-48 (3 DSPs) ■ PVDM2-64 (4 DSPs)	Sessions per PVDM: 8 16 32 48 64
NM-HD-1V	Fixed at 1 DSP	4 sessions per network module
NM-HD-2V	Fixed at 1 DSP	16 sessions per network module
NM-HD-2VE	Fixed at 3 DSPs	48 sessions per network module
WS-SVC-CMM-ACT	Fixed at 4 of Broadcom 1500	256 sessions per module

DSP Calculator


DSP Calculator - Cisco Systems - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl
Logged In | Contacts & Feedback | Help | Site Map | Select a Location / Language
Cisco Systems
Search
Products & Services | Ordering | Technical Support & Documentation | Learning & Events | Partners & Resellers | About C
HOME
TECHNICAL SUPPORT & DOCUMENTATION
TOOLS & RESOURCES
DSP Calculator
Tools & Resources
DSP Calculator
SELECT ROUTER
CONFIGURE ROUTER
CONFI OPTI
Toolkit: Roll over
Feedback | Help
Related Tools
IOS Upgrade Plan
1700 Series Desi
TAC Case Open
TAC Case Query
Related Links
Products & Serv
Cisco 1700 Series
Routers Introducti
Done
1
2

Select Router and Software Versions

Router Model: Cisco 2811

IOS Mainline Release: Select One (or)

IOS T Train Release: 12.4(6)T (or)

IOS Special Release: Select One

Next

Note : Releases displayed are valid for the platform selected.

1 Select the router model.

2 Select the Cisco IOS release.

DSP Calculator URL:
http://www.cisco.com/cgi-bin/Support/DSP/dsp-calc.pl

For easier DSP calculation, a DSP calculator tool is available at the following URL: http://www.cisco.com/cgi-bin/Support/DSP/dsp-calc.pl

This example shows how to calculate the required DSPs to deploy the following media resources on a single gateway:

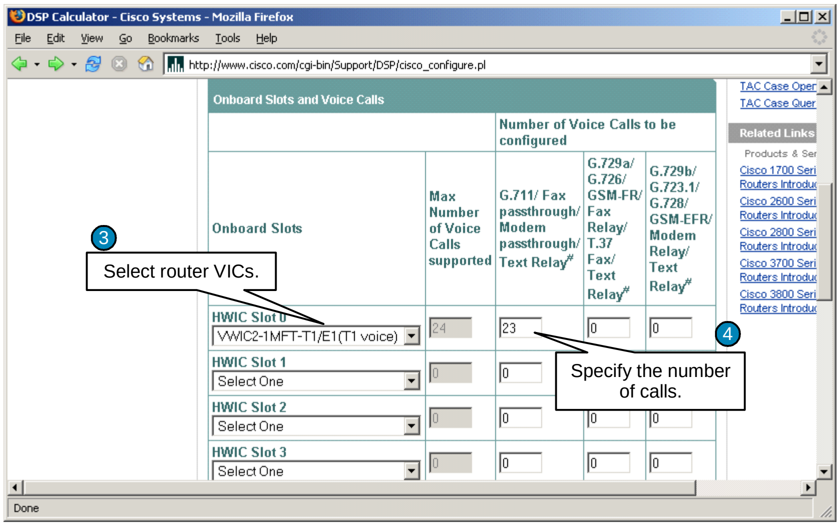
- **Router model:** Cisco 2811 Integrated Services Router
- **Cisco IOS release:** 12.4(6)T
- **Installed voice interface cards (VICs):** Onboard slot 0, VWIC2-1MFT-T1/E1 used as a PRI T1 with 23 voice bearer channels
- **Number of G.711 calls:** 23
- **Number of transcoding sessions:** Eight G.711 to G.729A
- **Number of conferences:** Four mixed-mode conferences

Follow these steps to do the calculation:

Step 1 Select the router model, in this case, Cisco 2811 Integrated Services Router.

Step 2 Select the Cisco IOS release: mainline release, T train release, or special release. In this case, 12.4(6)T is selected. Different Cisco IOS releases may lead to different DSP calculations because the firmware of a DSP is dependant on the Cisco IOS version used.

DSP Calculator (Cont.)



Onboard Slots and Voice Calls

Onboard Slots	Max Number of Voice Calls supported	Number of Voice Calls to be configured		
		G.711/ Fax passthrough/ Modem passthrough/ Text Relay#	G.729a/ G.726/ GSM-FR/ Fax Relay/ T.37 Fax/ Text Relay#	G.729b/ G.723.1/ G.728/ GSM-EFR/ Modem Relay/ Text Relay#
HWIC Slot 0 VWIC2-1MFT-T1/E1(T1 voice)	24	23	0	0
HWIC Slot 1 Select One	0	0		
HWIC Slot 2 Select One	0	0	0	0
HWIC Slot 3 Select One	0	0	0	0

Select router VICs.

Specify the number of calls.

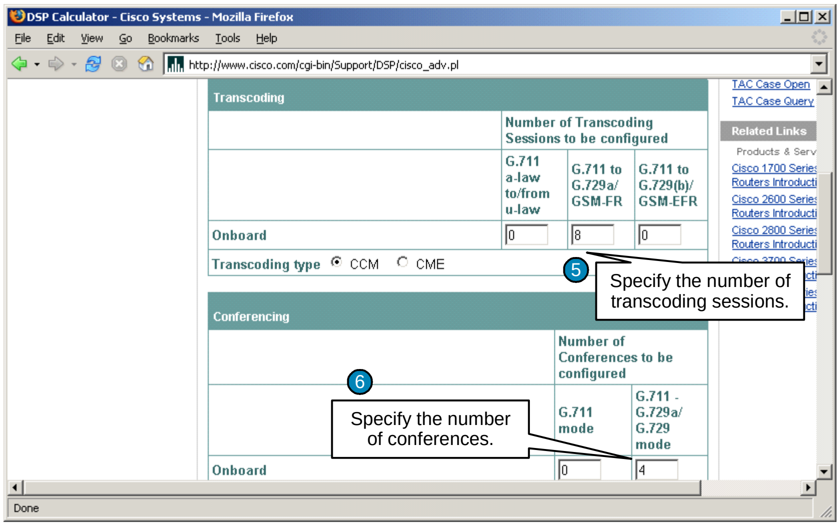
CVOICE v6.0—1-18

Step 3 Select the VIC configuration. In this case, a VWIC2-1MFT-T1/E1 (T1 voice) is selected. The T1 Voice option is necessary because the VWIC2 supports both E1 and T1.

Step 4 Specify the maximum number of calls for a specific codec or fax configuration. In this case, a full T1 is configured for PRI, that is, 23 G.711 calls.

Note A full T1 PRI supports only 23 voice channels. A T1 channel associated signaling (CAS) or a T1 configured for Non-Facility Associated Signaling (NFAS) can support up to 24 voice channels.

DSP Calculator (Cont.)


DSP Calculator - Cisco Systems - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.cisco.com/cgi-bin/Support/DSP/cisco_adv.pl
TAC Case Open
TAC Case Query
Related Links
Products & Serv
Cisco 1700 Series Routers Introducti
Cisco 2600 Series Routers Introducti
Cisco 2800 Series Routers Introducti
Done

Transcoding

	Number of Transcoding Sessions to be configured		
	G.711 a-law to/from u-law	G.711 to G.729a/ GSM-FR	G.711 to G.729(b)/ GSM-EFR
Onboard	0	8	0

Transcoding type ● CCM ○ CME

5 Specify the number of transcoding sessions.

Conferencing

	Number of Conferences to be configured	
	G.711 mode	G.711 - G.729a/ G.729 mode
Onboard	0	4

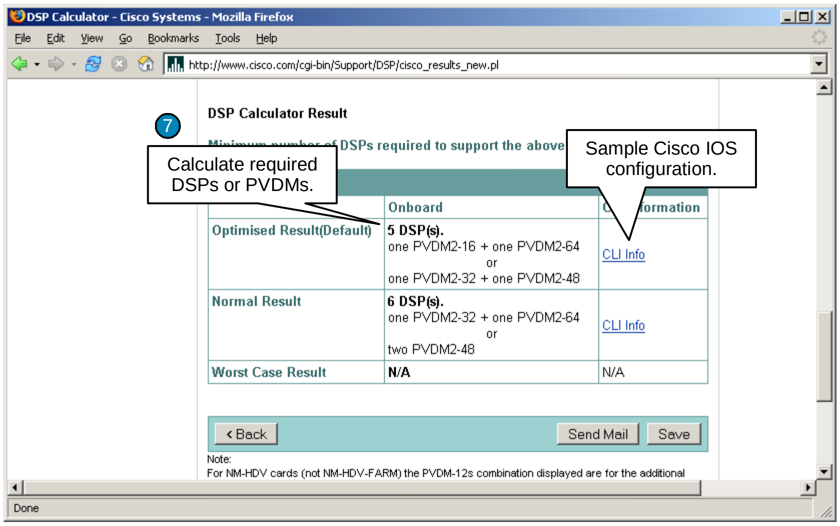
6 Specify the number of conferences.

CVOICE v6.0—1-19

Step 5 Specify the number of transcoding sessions with the appropriate codec. In this example, eight G.711 to G.729A sessions are required.

Step 6 Specify the number of either single-mode G.711 or mixed-mode conferences that are required on the gateway.

DSP Calculator Results



DSP Calculator - Cisco Systems - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.cisco.com/cgi-bin/Support/DSP/cisco_results_new.pl
7
&lt; Back
Send Mail
Save
Done

DSP Calculator Result

Minimum number of DSPs required to support the above

	Onboard	C formation
Optimised Result(Default)	**5 DSP(s).** one PVDM2-16 + one PVDM2-64 or one PVDM2-32 + one PVDM2-48	CLI Info
Normal Result	**6 DSP(s).** one PVDM2-32 + one PVDM2-64 or two PVDM2-48	CLI Info
Worst Case Result	**N/A**	N/A

Note:
For NM-HDV cards (not NM-HDV-FARM) the PVDM-12s combination displayed are for the additional

Calculate required DSPs or PVDMs.

Sample Cisco IOS configuration.

Step 7 After you enter all parameters, you can calculate the DSP resources. For our example, five C5510 DSPs need to be deployed, as shown in the “DSP Requirements” table.

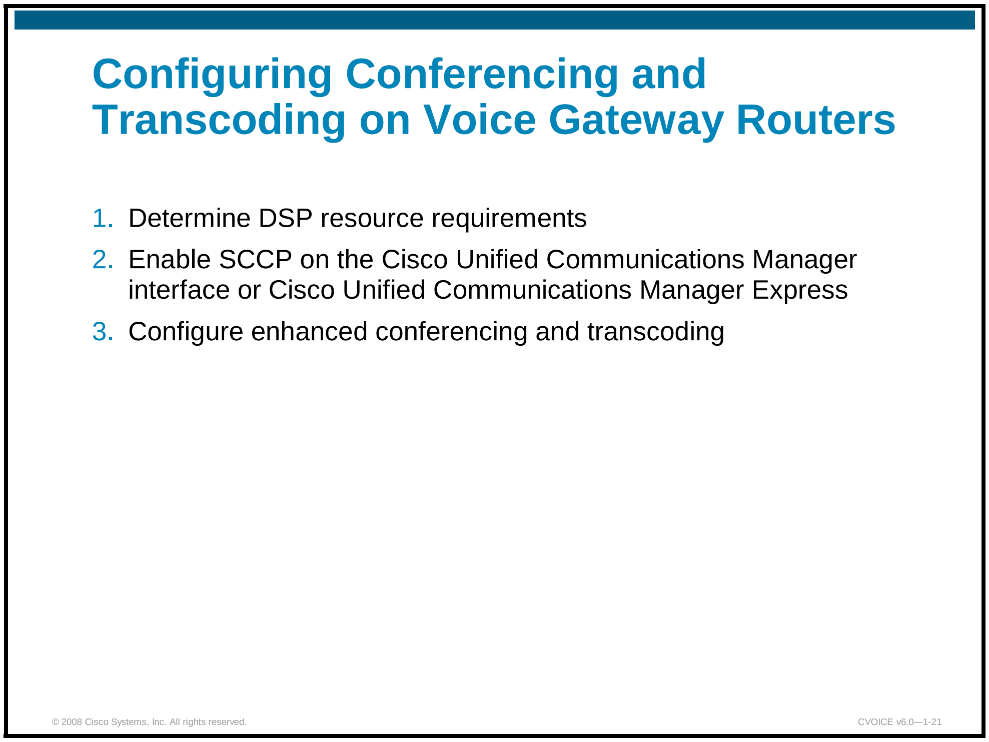
DSP Requirements

Media Resource	Number of DSPs
Voice termination for up to 23 G.711 calls	2 C5510
Transcoding for up to 8 G.729a sessions	1 C5510
4 conference bridges, each with up to 8 participants	2 C5510

Note The calculator displays two results: Optimized Result and Normal Result. The optimized result uses the C5510s in flex mode, and the normal result uses either medium- or high-complexity mode, depending on the codecs that are being used. You should use flex mode due to higher performance and fewer required DSP resources. In rare cases, this might lead to oversubscribed DSP resources.

Configuring Conferencing and Transcoding on Voice Gateways

This topic describes DSP farms, DSP farm profiles, and how to configure conferencing and transcoding on a voice gateway.



Configuring Conferencing and Transcoding on Voice Gateway Routers

1. Determine DSP resource requirements
2. Enable SCCP on the Cisco Unified Communications Manager interface or Cisco Unified Communications Manager Express
3. Configure enhanced conferencing and transcoding

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-21

The configuration of transcoding and conferencing on a voice gateway involves DSP resource requirements, Skinny Client Control Protocol (SCCP) configuration, DSP farm and DSP farm profile configuration, and hardware configurations.

The basic steps for configuring conferencing and transcoding on voice gateway routers are as follows:

1. **Determine DSP resource requirements:** DSPs reside either directly on a voice network module, such as the NM-HD-2VE, on PVDM2s that are installed in a voice network module, such as the NM-HDV2, or on PVDM2s that are installed directly onto the motherboard, such as on the Cisco 2800 and 3800 Series Integrated Services Routers. You must determine the number of PVDM2s or network modules that are required to support your conferencing and transcoding services and install the modules on your router.

2. **Enable SCCP on the Cisco Unified Communications Manager interface:** This step is beyond the scope of this course and will be covered in *Cisco IP Telephony Part 1*.

3. **Configure enhanced conferencing and transcoding:** Configuring conferencing and transcoding on the voice gateway includes the following substeps:

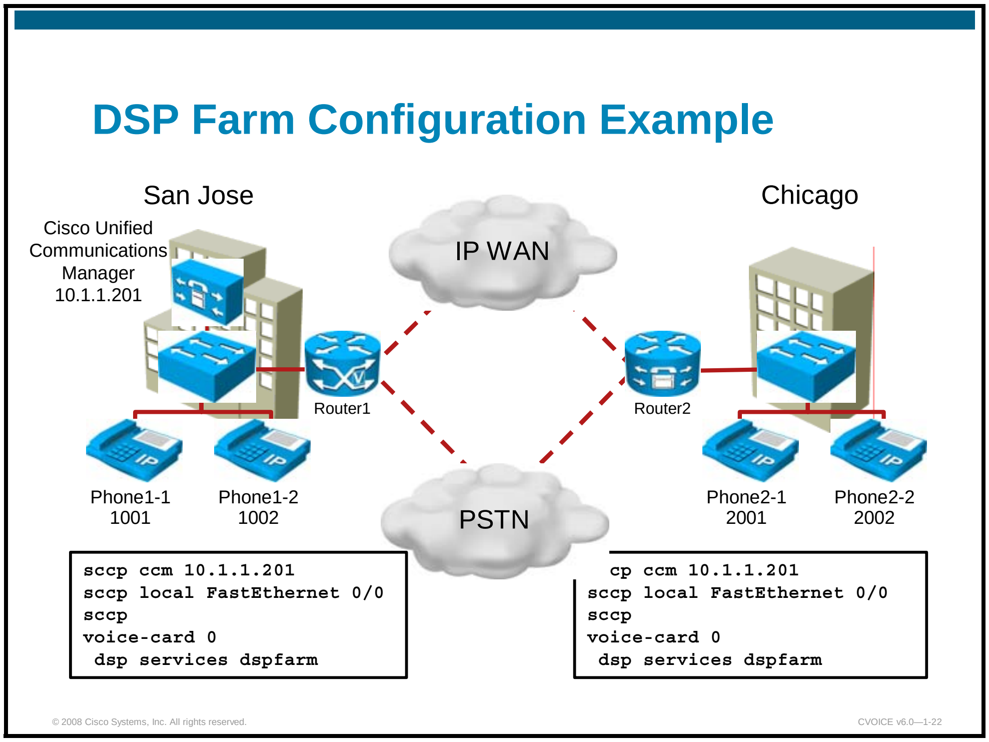
   — **Enable DSP farm services:** This substep is covered in next subtopic.

   — **Configure a DSP farm profile:** This substep is covered in the “DSP Profiles” subtopic.

- **Associate a DSP farm profile to a Cisco Unified Communications Manager group:** This step is beyond the scope of this course and will be covered in *Cisco IP Telephony Part 1*.
- **Verify DSP farm configuration:** This substep is covered in the “DSP Farm Configuration Commands for Enhanced Media Resources” topic.

DSP Farms

This subtopic describes DSP farms and how to enable DSP farm services.



DSP Farm Configuration Example

```
sccp ccm 10.1.1.201
sccp local FastEthernet 0/0
sccp
voice-card 0
 dsp services dspfarm
```

```
  cp ccm 10.1.1.201
sccp local FastEthernet 0/0
sccp
voice-card 0
 dsp services dspfarm
```

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—1-22

A DSP farm is the collection of DSP resources that are available for conferencing, transcoding, and MTP services. DSP farms are configured on the voice gateway and managed by Cisco Unified Communications Manager through SCCP.

The DSP farm can support a combination of transcoding sessions, MTP sessions, and conferences simultaneously. The DSP farm maintains the DSP resource details locally. Cisco Unified Communications Manager requests conferencing or transcoding services from the gateway, which either grants or denies these requests depending on resource availability. The details of whether DSP resources are used, and which DSP resources are used, are transparent to Cisco Unified Communications Manager.

The DSP farm uses the DSP resources in network modules on Cisco routers to provide voice conferencing, transcoding, and hardware MTP services.

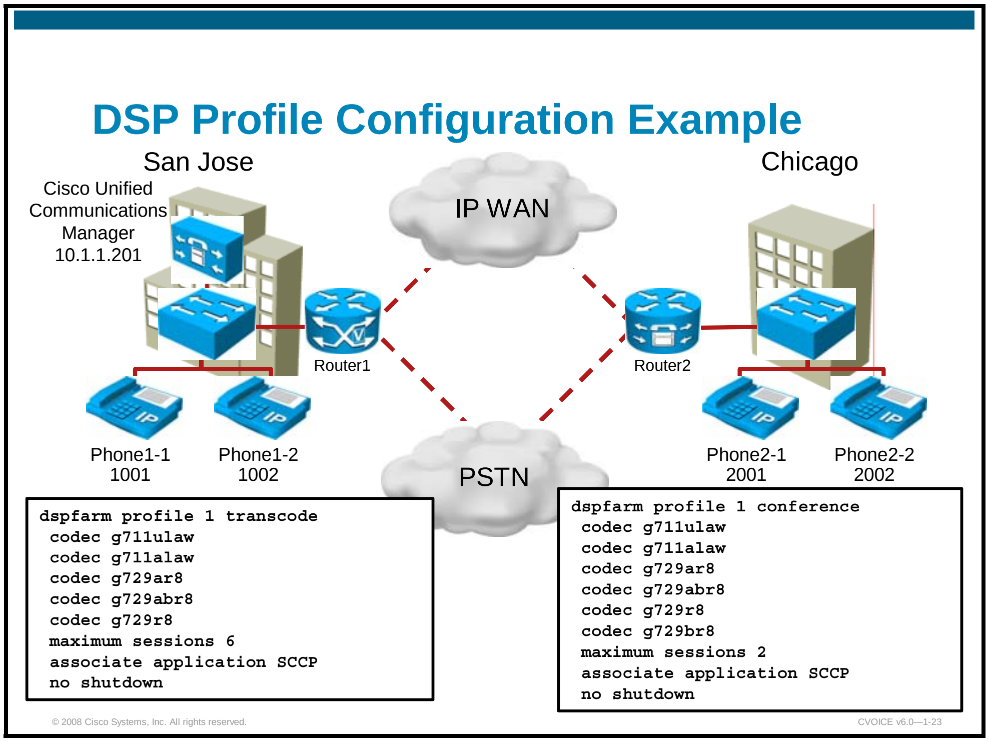
Configuration Example

Prior to actual media resource configuration, the DSPs need to be enabled for DSP farm usage. The **dsp services dspfarm** command allocates the DSPs to the DSP farm, and the **dspfarm** command enables the farm.

In the example above, the DSPs needed are enabled for DSP farm usage on both gateways, Router1 and Router2.

DSP Profiles

This subtopic covers DSP profiles and how to configure them.



DSP Profile Configuration Example

```
dspfarm profile 1 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 maximum sessions 6
 associate application SCCP
 no shutdown
```

```
dspfarm profile 1 conference
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 maximum sessions 2
 associate application SCCP
 no shutdown
```

CVOICE v6.0—1-23

DSP farm profiles are created to allocate DSP farm resources. Under the profile, you select the service type (conference, transcode, or MTP), associate an application, and specify service-specific parameters such as codecs and the maximum number of sessions. A DSP farm profile allows you to group DSP resources based on the service type. Applications associated with the profile, such as SCCP, can use the resources allocated under the profile. You can configure multiple profiles for the same service, each of which can register with one Cisco Unified Communications Manager group. The profile ID and service type uniquely identify a profile, allowing the profile to uniquely map to a Cisco Unified Communications Manager group that contains a single pool of Cisco Unified Communications Manager servers.

Configuration Example

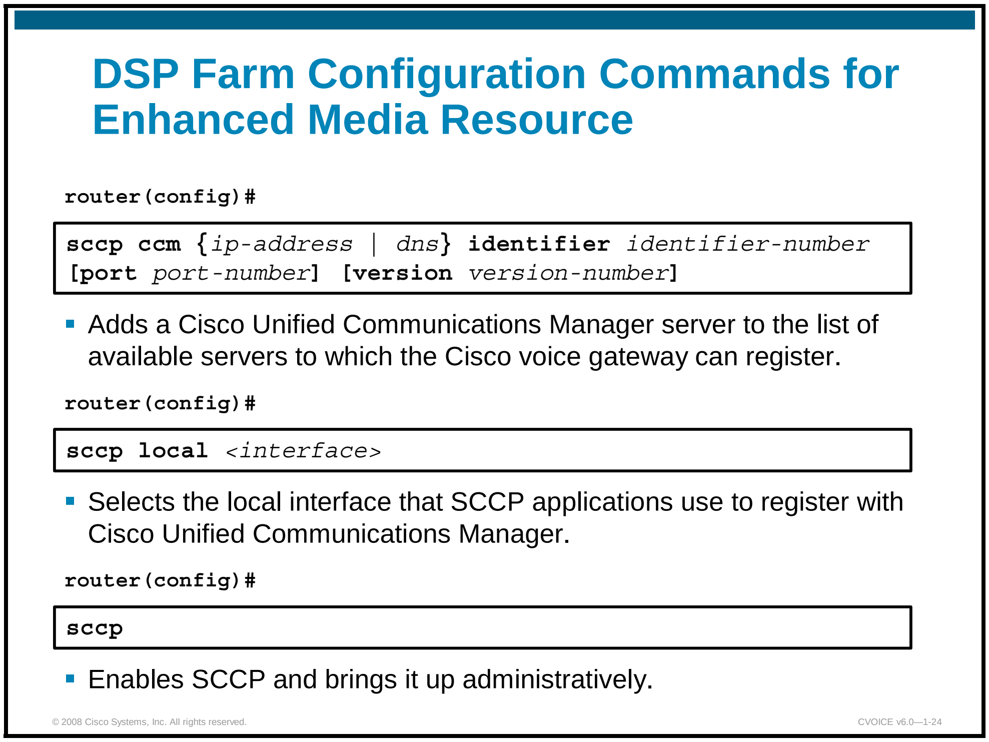
When the DSPs are ready, the DSP profile is configured using the **dspfarm profile** command. In the example above, because transcoding is required on Router1, the **dspfarm profile 1 transcoding** command is used. On Router2, the **dspfarm profile 1 conferencing** command creates a profile for conferencing.

Because both G.711 and G.729 are used in this deployment, multiple codecs are enabled on both the transcoding and conferencing profile using the **codec** *codec-type* command.

Note Because mixed-mode conferencing is configured, the two configured conferences require a full DSP. If only G.711 would be allowed, a single DSP on a PVDM2 would allow up to eight conferences.

DSP Farm Configuration Commands for Enhanced Media Resources

This topic describes the commands that are required to configure DSP farms on Cisco IOS gateways for enhanced media resources.



DSP Farm Configuration Commands for Enhanced Media Resource

```
router(config)#
```

```
sccp ccm {ip-address | dns} identifier identifier-number
[port port-number] [version version-number]
```

- Adds a Cisco Unified Communications Manager server to the list of available servers to which the Cisco voice gateway can register.

```
router(config)#
```

```
sccp local <interface>
```

- Selects the local interface that SCCP applications use to register with Cisco Unified Communications Manager.

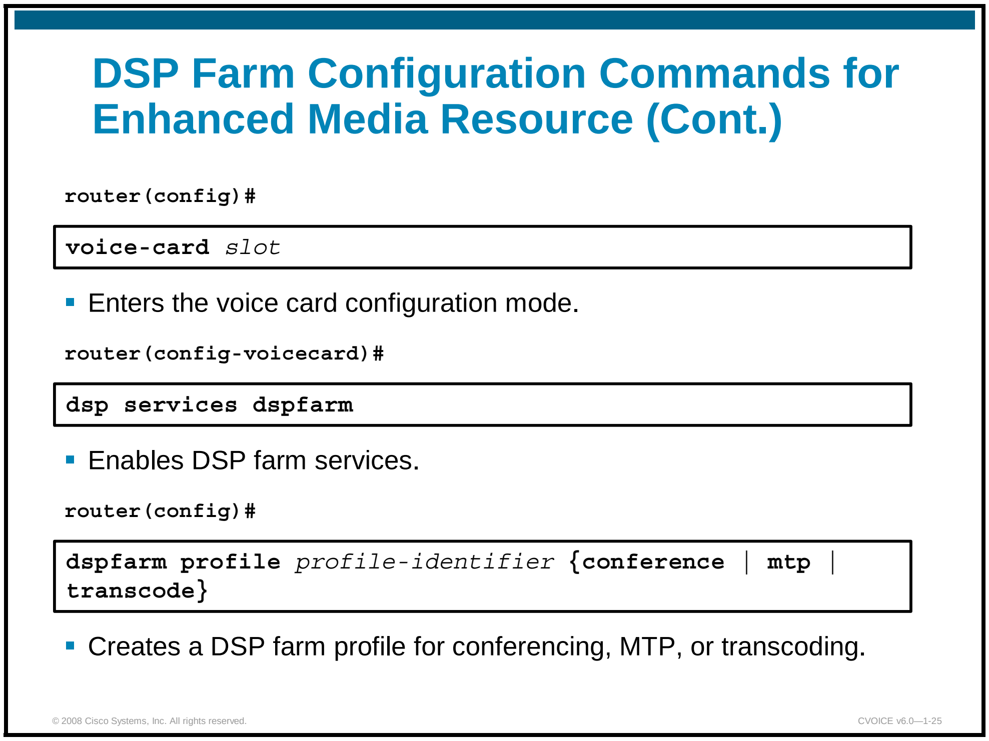
```
router(config)#
```

```
sccp
```

- Enables SCCP and brings it up administratively.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-24

Use the commands shown in the figure above to enable SCCP on the local interface that the voice gateway uses to communicate with Cisco Unified Communications Manager.



DSP Farm Configuration Commands for Enhanced Media Resource (Cont.)

```
router(config)#
```

```
voice-card slot
```

- Enters the voice card configuration mode.

```
router(config-voicecard)#
```

```
dsp services dspfarm
```

- Enables DSP farm services.

```
router(config)#
```

```
dspfarm profile profile-identifier {conference | mtp |
transcode}
```

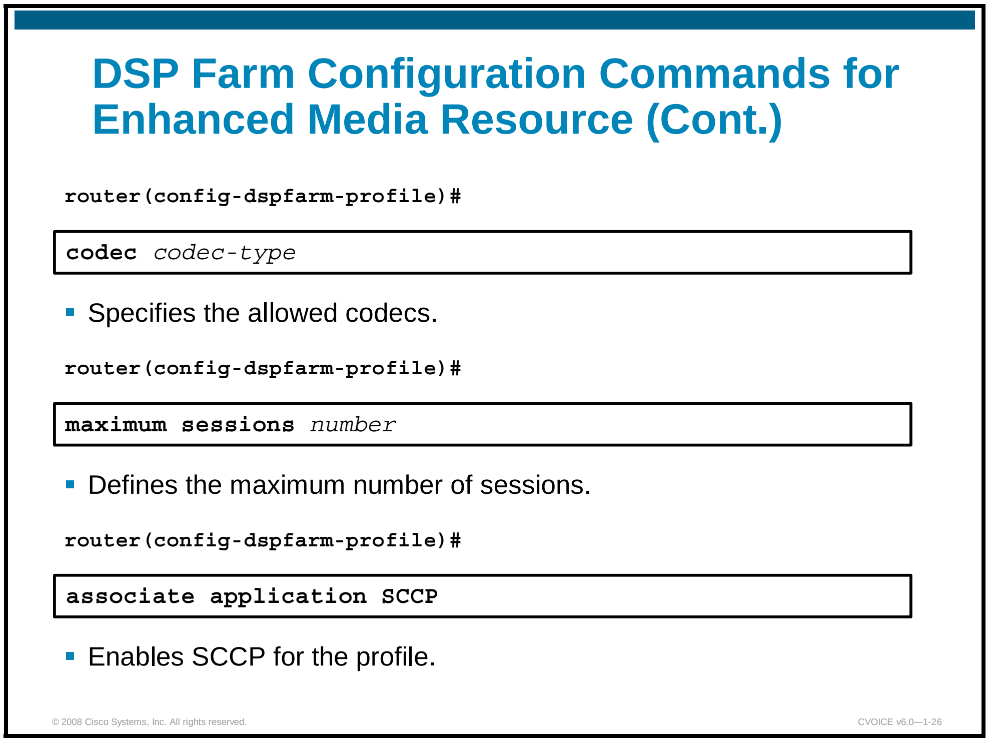
- Creates a DSP farm profile for conferencing, MTP, or transcoding.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-25

Prior to creating a DSP farm profile, you need to enable the DSPs for DSP services. You do this in the respective voice card configuration mode. After you have enabled DSPs for media resources, you can configure a DSP farm profile for conferencing or transcoding or as an MTP.

DSP Farm Configuration Commands

Command	Description
`voice-card` *`slot`*	To enter voice card configuration mode and configure a voice card, use the **voice-card** command in global configuration mode.
`dsp services dspfarm`	The router must be equipped with one or more voice network modules that provide DSP resources. DSP resources are used only if this command is configured under the particular voice card.
`dspfarm profile` *`profile-identifier`* **`{conference | mtp | transcode}`**	To enter DSP farm profile configuration mode and define a profile for DSP farm services, use the **dspfarm profile** command in global configuration mode. To delete a disabled profile, use the **no** form of this command. Use this command to create a new profile or to delete a disabled profile. If the profile is successfully created, the user enters the DSP farm profile configuration mode. Multiple profiles can be configured for the same service. If the profile is active, the user will not be allowed to delete the profile. The profile identifier uniquely identifies a profile. If the service type and profile identifier are not unique, a message is displayed that asks the user to choose a different profile identifier. You can choose the profile type by using one of these options: ■ To create a conference bridge, use the **conference** option. ■ To create a transcoder, use the **transcode** option. ■ To create a media termination point, use the **MTP** option.



DSP Farm Configuration Commands for Enhanced Media Resource (Cont.)

```
router(config-dspfarm-profile)#
```

```
codec codec-type
```

- Specifies the allowed codecs.

```
router(config-dspfarm-profile)#
```

```
maximum sessions number
```

- Defines the maximum number of sessions.

```
router(config-dspfarm-profile)#
```

```
associate application SCCP
```

- Enables SCCP for the profile.

CVOICE v6.0—1-26

Within the DSP farm configuration, you need to specify the supported codecs and maximum number of sessions. This configuration directly affects the number of required DSPs, so ensure that the configuration matches the design specifications.

You also need to associate the DSP farm profile with SCCP to operate correctly. This is done using the **associate application SCCP** command.

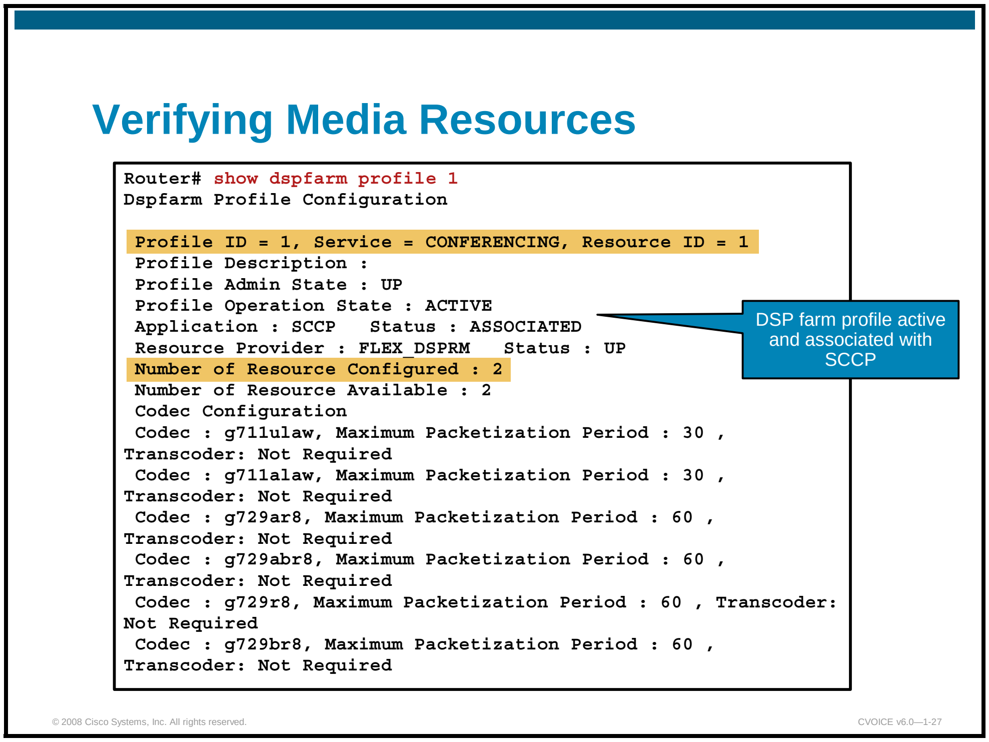
DSP Farm Configuration Commands

Command	Description
codec {*codec-type* | **pass-through**}	To specify the codecs supported by a DSP farm profile, use the **codec** command in DSP farm profile configuration mode. To remove the codec, use the **no** form of this command. Depending on the media resource, multiple codecs can be configured. Using higher complexity codecs, such as G.729, may decrease the number of sessions per DSP. Refer to the "DSP Requirements for Media Resources" topic for more information. The **pass-through** option is only available for MTPs and is typically used for Resource Reservation Protocol (RSVP)-based CAC that is controlled by Cisco Unified CallManager Release 5.0.
maximum sessions *number*	To specify the maximum number of sessions that are supported by the profile, use the **maximum sessions** command in DSP farm profile configuration mode. To reset to the default, use the **no** form of the command. For conferencing, the *number* actually specifies the number of conferences, not participants.

Command	Description
`associate profile sccp`	To associate the SCCP to the DSP farm profile, use the **associate application** command in DSP farm profile configuration mode. To remove the protocol, use the **no** form of this command. This association also requires a correct **sccp group** configuration to work correctly.

Verifying Media Resources

This topic describes how to verify the correct operation of available media resources.



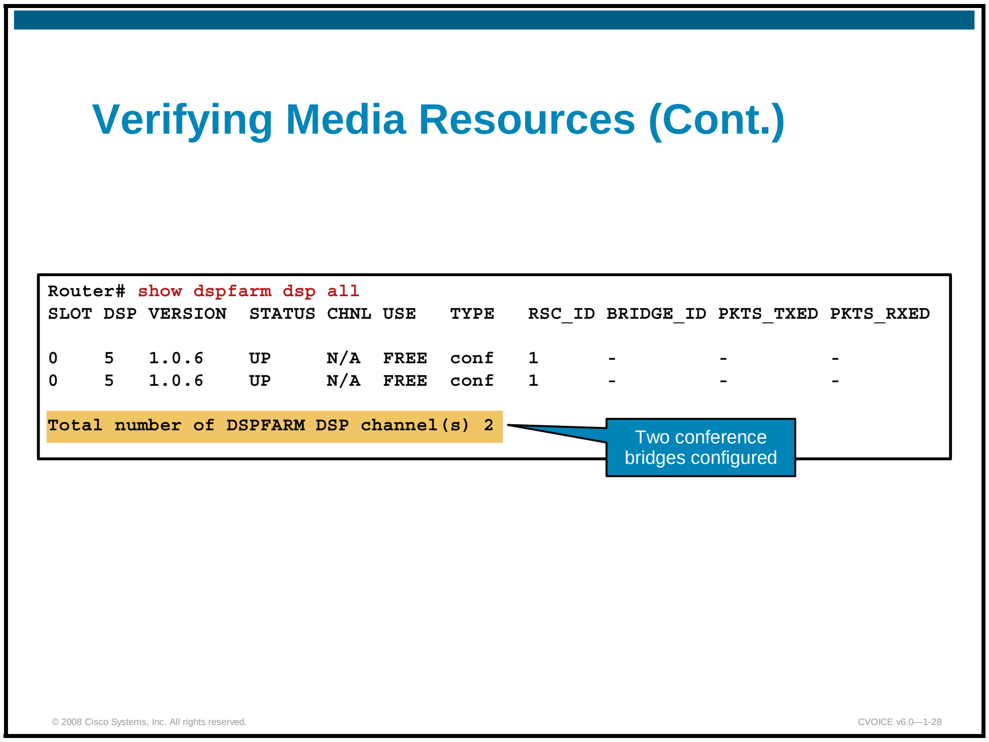
Verifying Media Resources

```
Router# show dspfarm profile 1
Dspfarm Profile Configuration

 Profile ID = 1, Service = CONFERENCING, Resource ID = 1
 Profile Description :
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resource Configured : 2
 Number of Resource Available : 2
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30 ,
Transcoder: Not Required
 Codec : g711alaw, Maximum Packetization Period : 30 ,
Transcoder: Not Required
 Codec : g729ar8, Maximum Packetization Period : 60 ,
Transcoder: Not Required
 Codec : g729abr8, Maximum Packetization Period : 60 ,
Transcoder: Not Required
 Codec : g729r8, Maximum Packetization Period : 60 , Transcoder:
Not Required
 Codec : g729br8, Maximum Packetization Period : 60 ,
Transcoder: Not Required
```

DSP farm profile active and associated with SCCP

CVOICE v6.0—1-27

To verify the configuration of a DSP farm profile, use the **show dspfarm profile** command. This output shows the DSP farm profile with ID 1 used for conferencing. Also note the Number of Resource Configured : 2 line, which is set by the **maximum session 2** command:



Verifying Media Resources (Cont.)

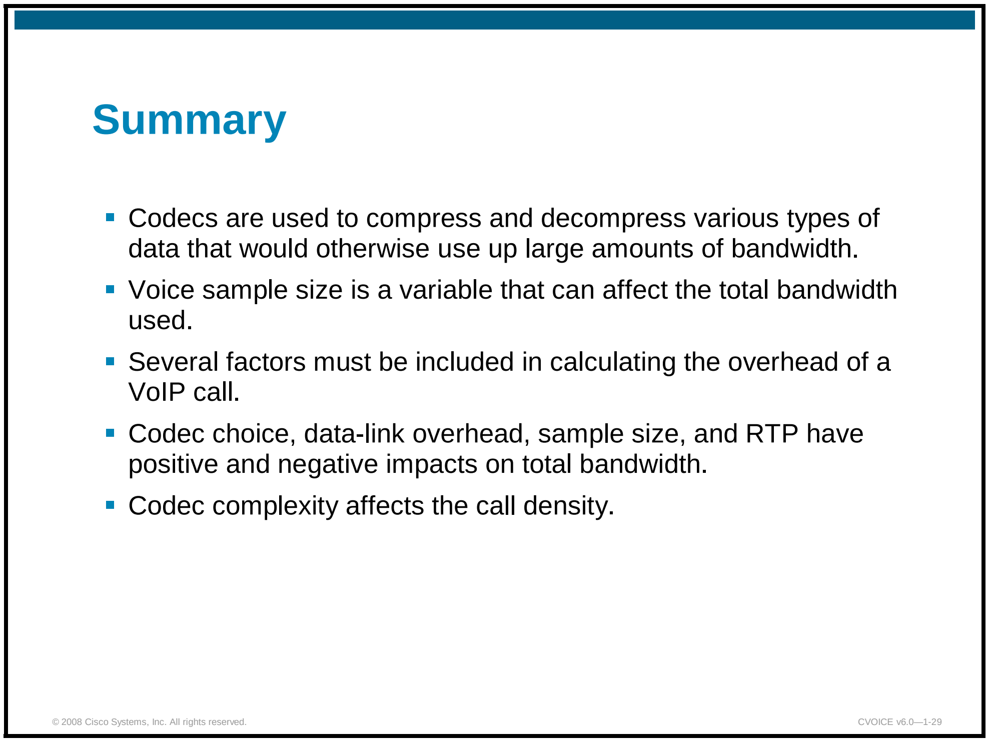
```
Router# show dspfarm dsp all
SLOT DSP VERSION  STATUS CHNL USE   TYPE   RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED

0    5   1.0.6    UP     N/A  FREE  conf   1      -         -         -
0    5   1.0.6    UP     N/A  FREE  conf   1      -         -         -

Total number of DSPFARM DSP channel(s) 2
```

Two conference bridges configured

To check the DSP status that was used for DSP farm profiles, use the **show dspfarm dsp all** command. This output shows two available DSPs that have been configured for conferencing:

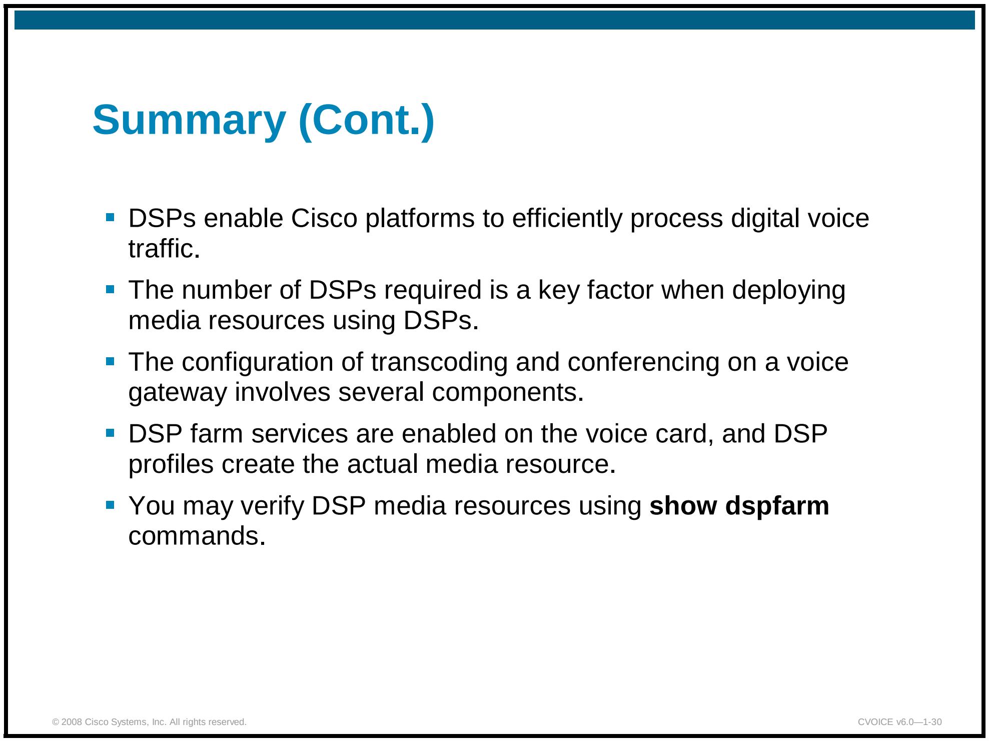
Summary

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



Summary

- Codecs are used to compress and decompress various types of data that would otherwise use up large amounts of bandwidth.
- Voice sample size is a variable that can affect the total bandwidth used.
- Several factors must be included in calculating the overhead of a VoIP call.
- Codec choice, data-link overhead, sample size, and RTP have positive and negative impacts on total bandwidth.
- Codec complexity affects the call density.



Summary (Cont.)

- DSPs enable Cisco platforms to efficiently process digital voice traffic.
- The number of DSPs required is a key factor when deploying media resources using DSPs.
- The configuration of transcoding and conferencing on a voice gateway involves several components.
- DSP farm services are enabled on the voice card, and DSP profiles create the actual media resource.
- You may verify DSP media resources using **show dspfarm** commands.

Lesson Self-Check

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

Q1) The _________ codec has the lowest bandwidth requirement?

Relates to: Codecs

Q2) Match the codec with the coding scheme that it uses.

Relates to: Codecs

A) G.711
B) G.726
C) G.728
D) G.729
E) G.723

_____ 1. ADPCM

_____ 2. CS-ACELP

_____ 3. LD-CELP

_____ 4. MPC-MLQ

_____ 5. PCM

Q3) One disadvantage of encapsulating more samples per PDU is that - ____________________________.

Relates to: Impact of Voice Samples and Packet Size on Bandwidth

Q4) The size of a voice sample from Cisco voice equipment using a G.728 codec is ______

Relates to: Impact of Voice Samples and Packet Size on Bandwidth

Q5) The overhead for Frame Relay is ____.

Relates to: Calculating Overhead

Q6) _____________ in the Ethernet II overhead are used for CRC.

Relates to: Calculating Overhead

Q7) The overhead associated with IPsec is _____________

Relates to: Calculating Overhead

Q8) The overhead associated with MPLS is ____________.

Relates to: Calculating Overhead

Q9) Which three factors must be considered when you are calculating the total bandwidth of a VoIP call? (Choose three.)

Relates to: Calculating the Total Bandwidth for a VoIP Call

A) codec size
A) CRC usage
B) network link overhead
C) sample size
D) capacity of network links
E) cpu size

Q10) The total bandwidth that is required for a 40-byte voice sample size that uses a G.729 codec and Frame Relay without cRTP is _______________.

Relates to: Calculating the Total Bandwidth for a VoIP Call

Q11) The formula used to calculate total bandwidth is ________________________________.

Relates to: Calculating the Total Bandwidth for a VoIP Call

Q12) The function of CNG is to ____.

Relates to: Calculating the Total Bandwidth for a VoIP Call

Q13) The bandwidth required if VAD is used when a voice call over Frame Relay is 11,395 b/s is ______________.

Relates to: Calculating the Total Bandwidth for a VoIP Call

Lesson Self-Check Answer Key

Q1) G.723

Q2) 1-B, 2-D, 3-C, 4-E, 5-A

Q3) the delay becomes more variable

Q4) 20 ms

Q5) 6 bytes

Q6) 4 bytes

Q7) 4 to 6 bytes

Q8) 24 bytes

Q9) A, C, D

Q10) 17,200 b/s

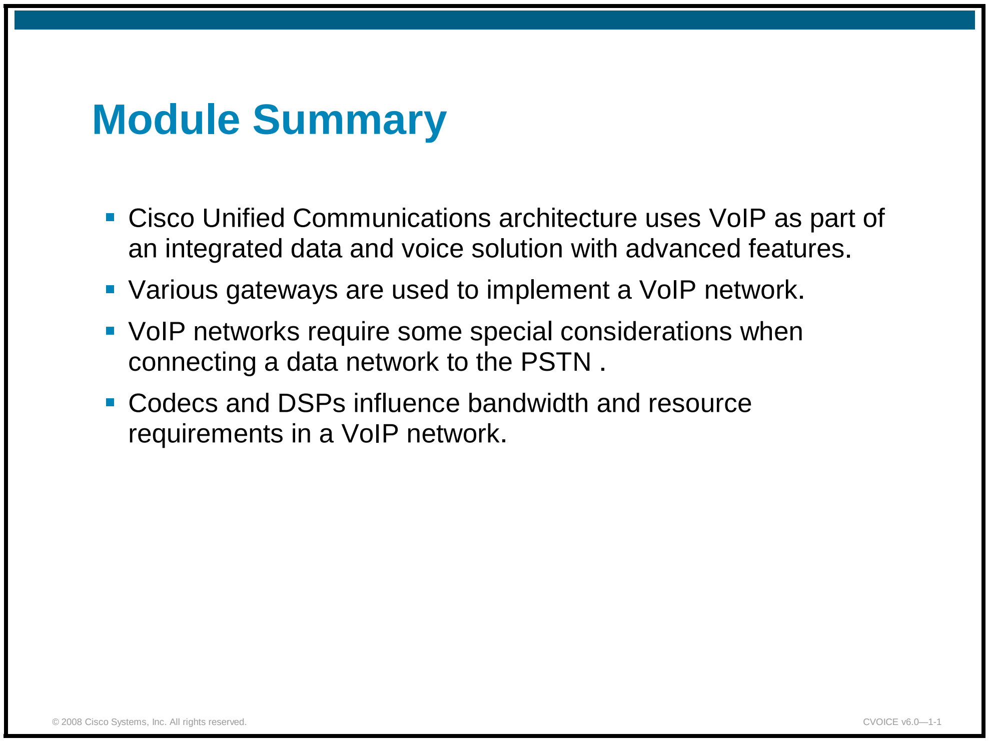
Q11) Total_Bandwidth = total packet size in bits * packets per second (PPS)

Q12) provide white noise to make the call sound connected

Q13) 7407 b/s

Module Summary

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



Module Summary

- Cisco Unified Communications architecture uses VoIP as part of an integrated data and voice solution with advanced features.
- Various gateways are used to implement a VoIP network.
- VoIP networks require some special considerations when connecting a data network to the PSTN .
- Codecs and DSPs influence bandwidth and resource requirements in a VoIP network.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—1-1

Successful VoIP integration into an existing data network requires that you have some very specific knowledge relating to VoIP technologies and gateways. This module introduced the Cisco Unified Communications architecture as well as VoIP. The module covered the common VoIP protocols that are used in a current VoIP network. The module also described various service considerations that must be observed when you are integrating a VoIP network into an exiting IP network. The module then covered gateways and how they are used in an IP telephony environment. The module covered special requirements for VoIP calls and ended with a discussion on codecs and digital signal processors (DSPs)and how they can impact a VoIP network.

References

For additional information, refer to these resources:

- Internet Engineering Task Force. RFCs 1889, 2508, 2509, 2543, 2545, 2705, 3261, 3550, 3665, and 3711. http://www.ietf.org/rfc.html.
- ITU. ITU G series recommendations. http://www.itu.int/rec/T-REC-g.
- ITU. ITU P series recommendations. http://www.itu.int/rec/T-REC-P.
- Cisco Systems, Inc. *Cisco Voice Gateways and Gatekeepers, Cisco Press.*
- Cisco Systems, Inc. Cisco IOS Voice Configuration Library. http://www.cisco.com/en/US/products/ps6441/prod_configuration_guide09186a0080565f8a.html.

- Cisco Systems, Inc. Unified Communications. *http://www.cisco.com/en/US/netsol/ns151/networking_solutions_unified_communications_home.html*.
- Cisco Systems, Inc. *Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 6.x.* http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a008085eb0d.html.
- Cisco Systems, Inc. Products & Services. http://www.cisco.com/en/US/products/sw/voicesw/index.html.
- Cisco Systems, Inc. Cisco Unified Communications Manager documentation. http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm.
- PESQ. News about PESQ. http://www.pesq.org.
- Cisco Systems, Inc. *Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms).*http://www.cisco.com/warp/public/788/voice-qos/jitter_packet_voice.html.
- Cisco Systems, Inc. *Understanding Delay in Packet Voice Networks.* http://www.cisco.com/warp/public/788/voip/delay-details.html.
- Cisco Systems, Inc. *Cisco IOS Fax and Modem Services over IP Application Guide.*http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a0080762024.html.
- Cisco Systems, Inc. *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4T.* http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/tqos_c/index.htm.
- Cisco Systems, Inc. *Introduction to QoS Features for Voice.* http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt7/qcfvoice.htm.
- Cisco Systems, Inc. *Voice Quality*. http://www.cisco.com/en/US/tech/tk652/tk698/tsd_technology_support_protocol_home.html.
- Cisco Systems, Inc. Voice codec bandwidth calculator. http://tools.cisco.com/Support/VBC/do/CodecCalc1.do
- Cisco Systems, Inc. *Voice over IP - Per Call Bandwidth Consumption*. http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html.
- Cisco Systems, Inc. *Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers.* http://www.cisco.com/en/US/partner/products/ps6441/products_configuration_guide_chapter09186a0080541bf3.html.
- Cisco Systems, Inc. *Cisco IOS Voice Troubleshooting and Monitoring Guide*. http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_troubleshooting_guide_chapter09186a0080558500.html.

Module 2

Voice Port Configuration

Overview

One of the most important aspects of any IP telephony deployment is its connection to phones, fax machines, the corporate WAN, and the public switched telephone network (PSTN). Another aspect that needs to be considered is the integration with existing PBX equipment to allow for a migration. Connecting voice devices to a network infrastructure requires an in-depth understanding of the signaling and electrical characteristics that are specific to each type of interface. After the configuration of physical ports on a gateway, you must then create some dial peers in order to complete calls that utilize the analog and digital ports. This module discusses the various technologies that are available for analog and digital connections and how to configure each of them. It also presents dial peers and how they are used within VoIP.

Module Objectives

Upon completing this module, you will be able to configure gateway interconnections to support VoIP and PSTN calls and to integrate with a PSTN and PBX. This ability includes being able to meet these objectives:

- Describe the various call types in a VoIP network
- Describe the various analog voice interfaces and how to configure them
- Describe the purpose and use of dial peers in VoIP
- Describe the various digital interfaces and how to configure them
- Describe QSIG and how to enable QSIG support

Lesson 1

Understanding Call Types

Overview

There are several call types that are used in a VoIP network. Knowing which types of calls will occur on the network is essential to designing and operating VoIP networks, and knowing the call types that influence dialing plans is useful when you are troubleshooting calls through a VoIP network. This lesson describes the types of calls that are typical in a VoIP environment.

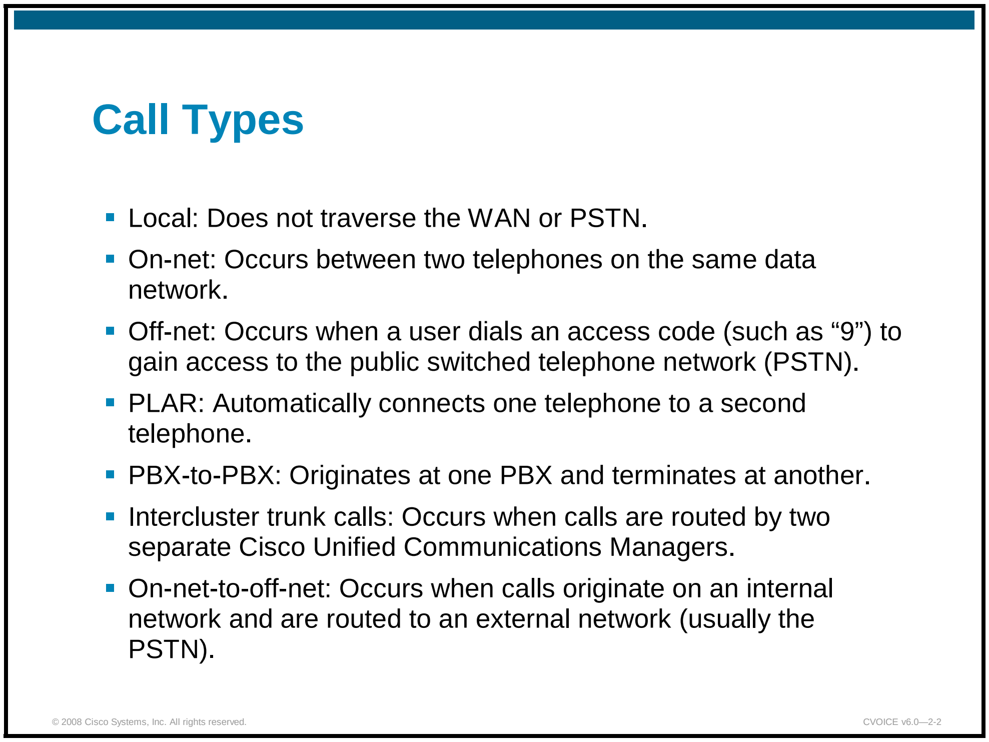
Objectives

Upon completing this lesson, you will be able to describe the various call types in a VoIP network. This ability includes being able to meet these objectives:

- List the seven call types in a VoIP network
- Describe the local call type
- Describe the on-net call type
- Describe the off-net call type
- Describe the PLAR call type
- Describe the PBX-to-PBX call type
- Describe the intercluster trunk call type
- Describe the on-net-to-off-net call type

Call Types

This topic describes each of the seven call types.



Call Types

- Local: Does not traverse the WAN or PSTN.
- On-net: Occurs between two telephones on the same data network.
- Off-net: Occurs when a user dials an access code (such as “9”) to gain access to the public switched telephone network (PSTN).
- PLAR: Automatically connects one telephone to a second telephone.
- PBX-to-PBX: Originates at one PBX and terminates at another.
- Intercluster trunk calls: Occurs when calls are routed by two separate Cisco Unified Communications Managers.
- On-net-to-off-net: Occurs when calls originate on an internal network and are routed to an external network (usually the PSTN).

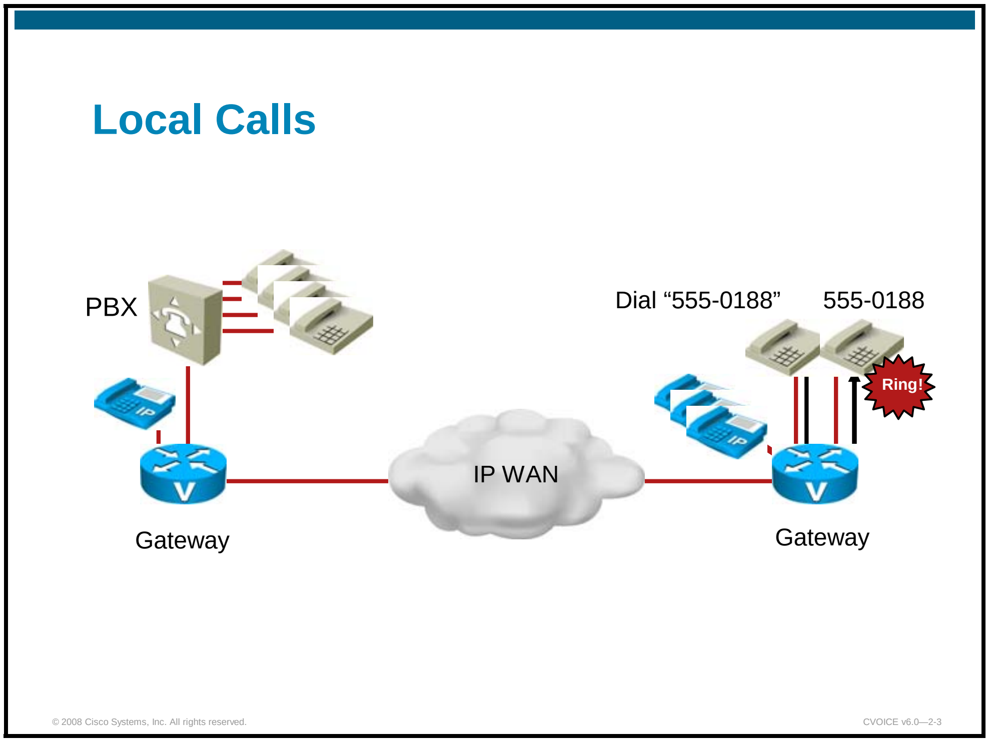
© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-2

The seven types of calls are:

- **Local calls:** A local call occurs between two devices that are connected to a single voice gateway. The call does not traverse the WAN or public switched telephone network (PSTN).
- **On-net calls:** An on-net call occurs between two telephones on the same network.
- **Off-net calls:** An off-net call occurs when a user dials an access code (such as 9) from a telephone that is directly connected to a Cisco voice-enabled router or PBX to gain access to the PSTN.
- **Private line, automatic ringdown (PLAR) calls:** A PLAR call automatically connects one telephone to a second telephone at another location.
- **PBX-to-PBX calls:** A PBX-to-PBX call originates at one PBX and terminates at another.
- **Intercluster trunk calls:** Intercluster trunk calls occur when a device that is controlled by one Cisco Unified Communications Manager calls another device that is controlled by another Cisco Unified Communications Manager.
- **On-net-to-off-net calls:** On-net-to-off-net calls occur when calls originate on an internal network and are routed to an external network (usually the PSTN).

Local Calls

This topic describes the local call type.



Local Calls

CVOICE v6.0—2-3

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.

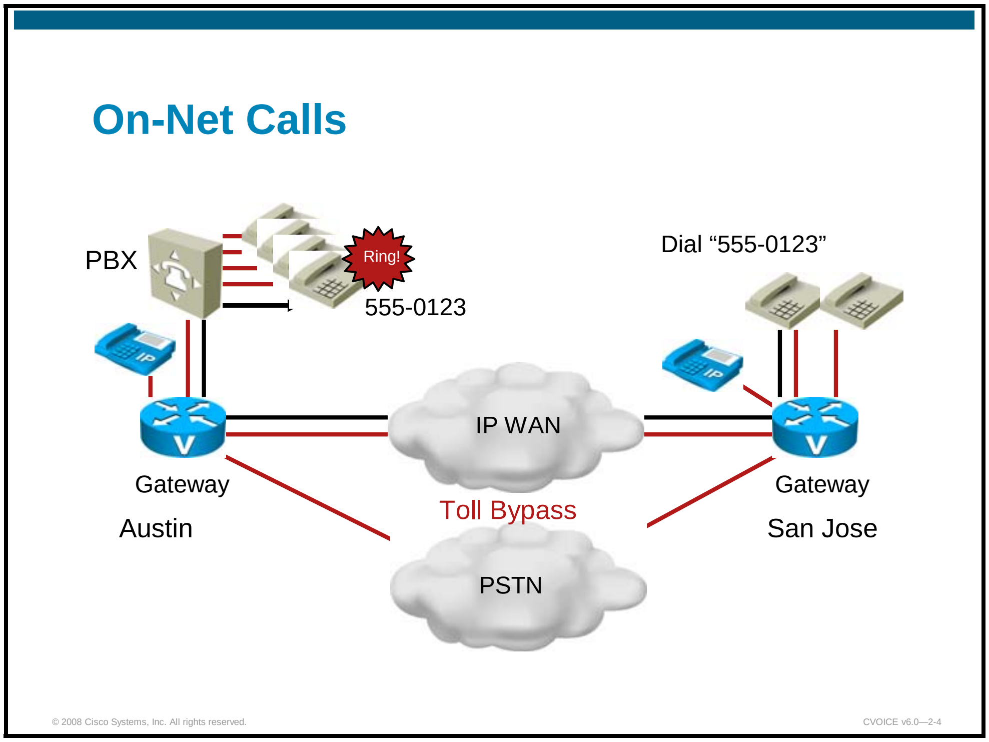
In the example in the figure, local calls occur between two telephones that are connected to one Cisco voice-enabled router. This type of call is handled entirely by the router and does not travel over an external network. Both telephones are directly connected to Foreign Exchange Station (FXS) ports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

Example

An example of a local call is one staff member calling another staff member at the same office. This call is switched between two ports on the same voice-enabled router.

On-Net Calls

This topic describes the on-net call type.



On-Net Calls

CVOICE v6.0—2-4

On-net calls are connected between two telephones on the same network. The calls can be routed through one or more Cisco voice-enabled routers, but the calls remain on the same network. The edge telephones attach to the network through direct connections and FXS ports, or through a PBX, which typically connects to the network via a T1 connection. IP phones that connect to the network via switches place on-net calls either independently or through the administration of Cisco Unified Communications Manager. 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.

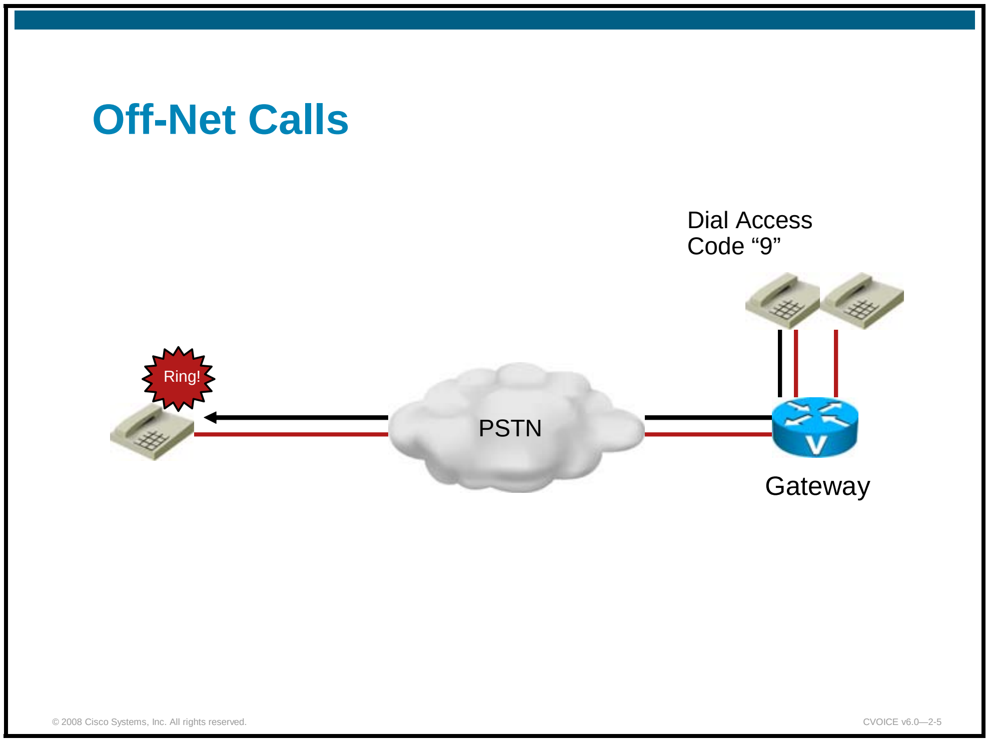
Note The act of routing voice data across the WAN instead of across the PSTN is known as toll bypass. Originally, companies saved significant amounts of money using this strategy, which was one of the first major business benefits of a VoIP-enabled network.

Example

An example of an on-net call is one staff member calling another staff member at a remote office. The call is sent from the local voice-enabled router across the IP network and is terminated on the remote office voice-enabled router.

Off-Net Calls

This topic describes the off-net call type.



Off-Net Calls

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-5

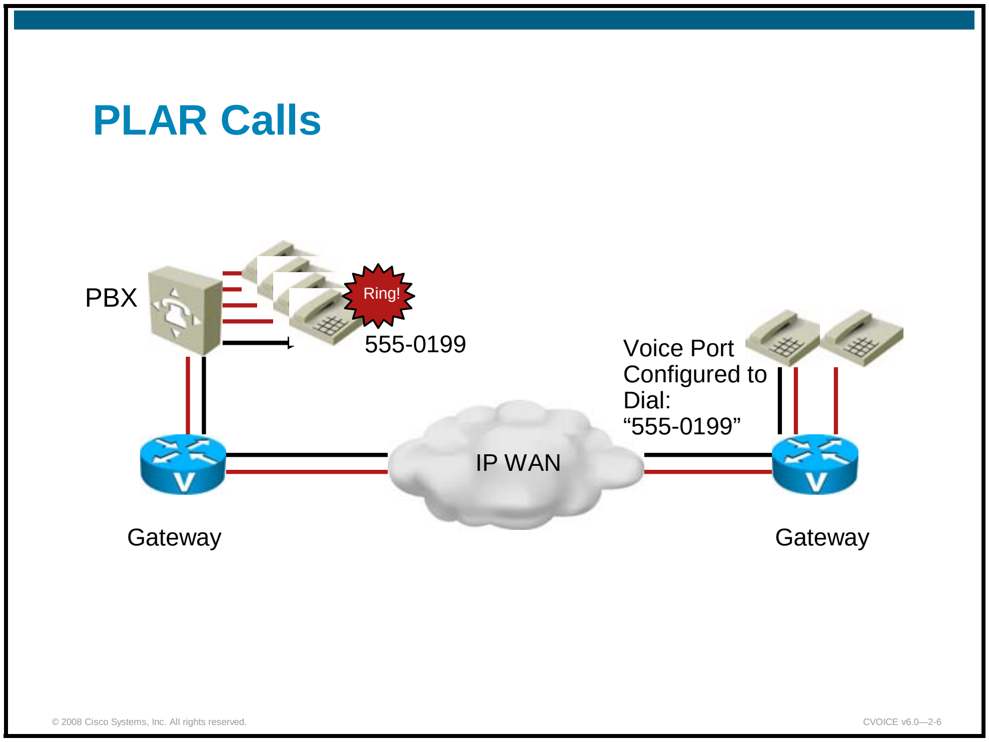
An off-net call occurs when a user dials an access code (such as 9) from a telephone that is directly connected to a Cisco voice-enabled router or PBX to gain access to the PSTN. The connection to the PSTN is a single analog connection via a Foreign Exchange Office (FXO) port or a digital T1 or E1 connection.

Example

An example of an off-net call is a staff member calling a client who is located in the same city. The call is sent from the local voice-enabled router that is acting as a gateway to the PSTN. The call is then sent to the PSTN for call termination.

PLAR Calls

This topic describes the PLAR call type.



PLAR Calls

CVOICE v6.0—2-6

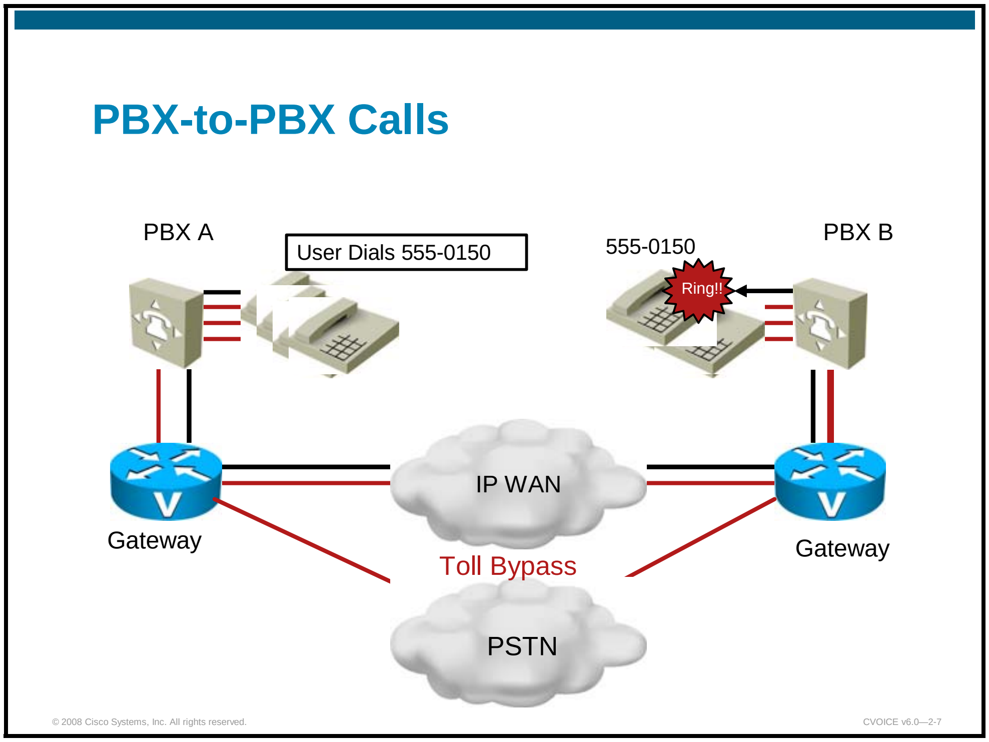
PLAR calls automatically connect one telephone to a second telephone when the first telephone goes off hook. When this connection occurs, the user does not get a dial tone because the voice-enabled port for that telephone is preconfigured with a specific number to dial. A PLAR connection can work between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

Example

An example of a PLAR call is a client picking up a customer service telephone located in the lobby of the office and being automatically connected to a customer service representative without dialing any digits. The call is automatically dialed, based on the PLAR configuration of the voice port. In this case, as soon as the handset goes off hook, the voice-enabled router generates the preconfigured digits to place the call.

PBX-to-PBX Calls

This topic describes the PBX-to-PBX call type.



PBX-to-PBX Calls

CVOICE v6.0—2-7

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

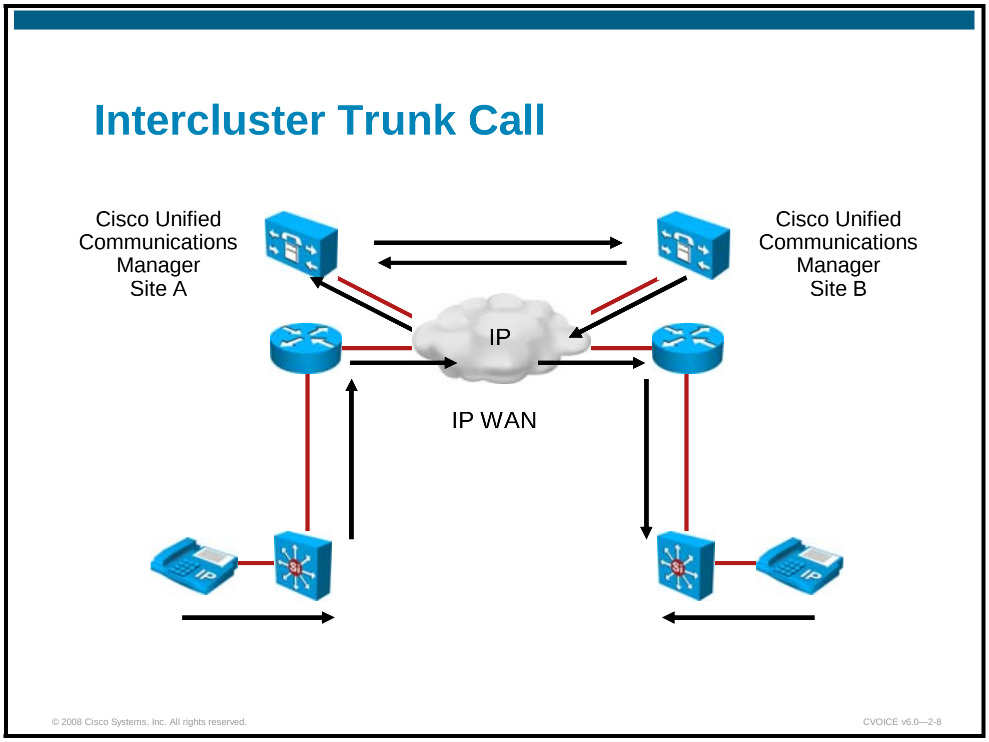
Note This call type is another form of toll bypass.

Example

An example of a PBX-to-PBX call is one staff member calling another staff member at a remote office. The call is sent from the local PBX, through a voice-enabled router, across the IP network, and through the remote voice-enabled router, and is terminated on the remote office PBX.

Intercluster Trunk Calls

This topic describes the intercluster trunk call type.



Intercluster Trunk Call

Cisco Unified Communications Manager Site A
Cisco Unified Communications Manager Site B
IP
IP WAN

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-8

As part of an overall migration strategy, a business may replace PBXs, including IP phones that are connected to the IP network, with Cisco Unified Communications Manager. Cisco Unified Communications Manager performs the call-routing functions that were formerly provided by the PBX. When an IP phone call is placed using a configured Cisco Unified Communications Manager, the call is assessed to see if the call is destined for another IP phone under its control or if the call must be routed through a remote Cisco Unified Communications Manager for call completion. Intercluster trunk calls are routed between Cisco Unified Communications Manager clusters using a trunk.

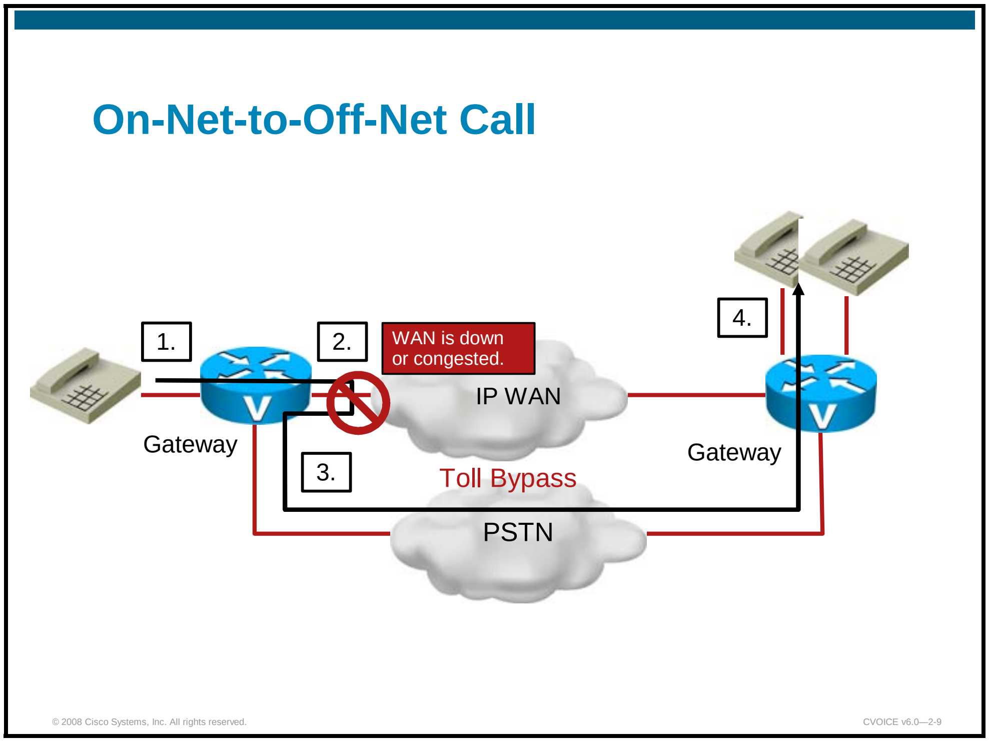
Example

An example of an intercluster trunk call is one staff member calling another staff member at a remote office using an IP phone. The call setup is handled by the Cisco Unified Communications Manager devices at each location. After the call is set up, the IP phones generate Real-Time Transport Protocol (RTP) packets that carry voice data between sites.

Note Cisco Unified Communications Manager is examined in detail in the *Cisco IP Telephony* courses.

On-Net-to-Off-Net Calls

This topic describes the on-net-to-off-net call type.



On-Net-to-Off-Net Call

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—2-9

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

Note	On-net-to-off-net calls may occur as a result of dial plan configuration, or they may be redirected by Call Admission Control (CAC).

Example

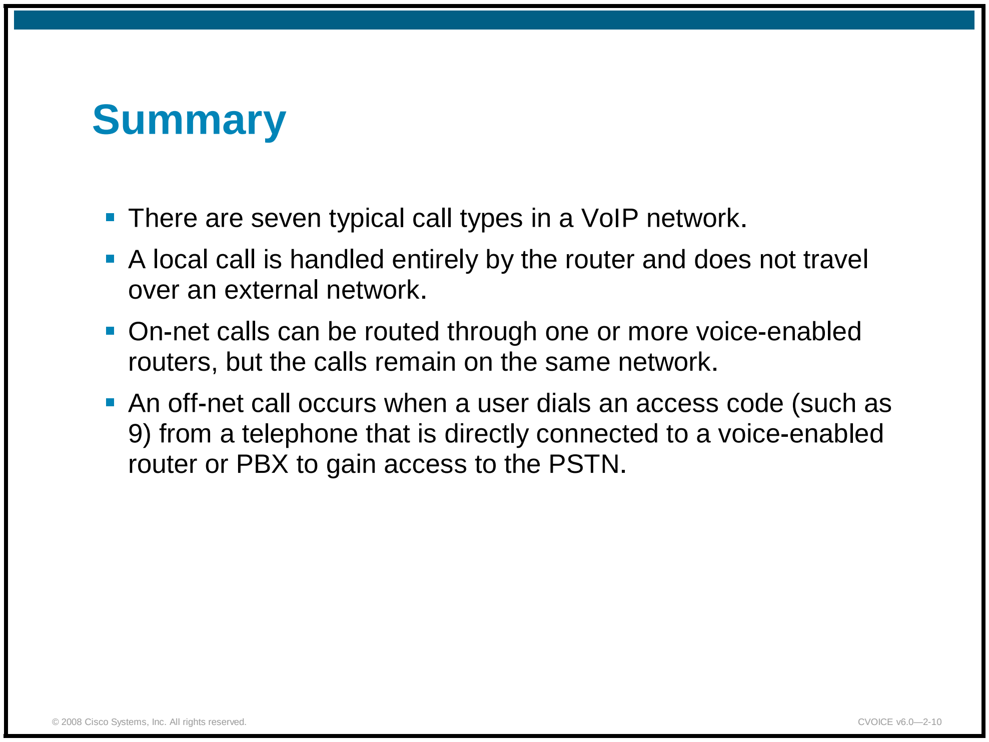
An example of an on-net-to-off-net call is one staff member calling another staff member at a remote office while the WAN link is congested. When the originating voice-enabled router determines that it cannot terminate the call across the WAN link, it sends the call to the PSTN with the appropriate dialed digits to terminate the call at the remote office via the PSTN network.

Call flow of an on-net-to-off-net call follows:

1. A user on the network initiates a call to a remote site.
2. The output of the WAN gateway is either down or congested, so the call is rerouted.
3. The call connects to the PSTN.
4. The PSTN completes the call to the remote site.

Summary

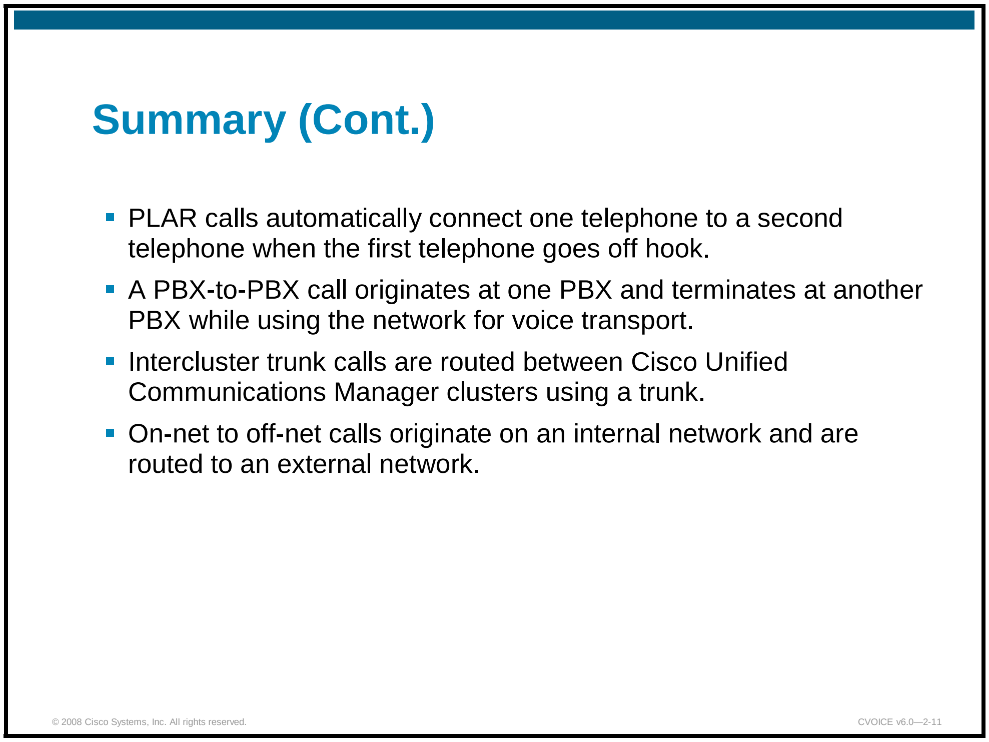
This topic summarizes the key points that were discussed in this lesson.



Summary

- There are seven typical call types in a VoIP network.
- A local call is handled entirely by the router and does not travel over an external network.
- On-net calls can be routed through one or more voice-enabled routers, but the calls remain on the same network.
- An off-net call occurs when a user dials an access code (such as 9) from a telephone that is directly connected to a voice-enabled router or PBX to gain access to the PSTN.

CVOICE v6.0—2-10



Summary (Cont.)

- PLAR calls automatically connect one telephone to a second telephone when the first telephone goes off hook.
- A PBX-to-PBX call originates at one PBX and terminates at another PBX while using the network for voice transport.
- Intercluster trunk calls are routed between Cisco Unified Communications Manager clusters using a trunk.
- On-net to off-net calls originate on an internal network and are routed to an external network.

CVOICE v6.0—2-11

Lesson Self-Check

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

Q1) There are _________ typical call types in a VoIP network.

Relates to: Call Types

Q2) A local call is handled entirely by the _____ and does not travel over an external network.

Relates to: Local Calls

Q3) On-net calls can be routed through one or more voice-enabled routers, but the calls remain on the same _____.

Relates to: On-Net Calls

Q4) An off-net call occurs when a user dials _____from a telephone that is directly connected to a voice-enabled router or PBX to gain access to the PSTN.

Relates to: Off-Net Calls

Q5) PLAR calls automatically connect one telephone to a second telephone when the first telephone goes _____.

Relates to: PLAR Calls

Q6) A PBX-to-PBX call originates at one PBX and terminates at another PBX while using the _____ for voice transport.

Relates to: PBX-to-PBX Calls

Q7) Intercluster trunk calls are routed between _____ using a trunk.

Relates to: Intercluster Trunk Calls

Q8) On-net-to-off-net calls originate on _____ and are routed to an external network.

Relates to: On-Net-to-Off-Net Calls

Lesson Self-Check Answer Key

Q1) seven

Q2) router

Q3) network

Q4) an access code

Q5) off hook

Q6) network

Q7) Cisco Unified Communications Manager clusters

Q8) an internal network

Lesson 2

Configuring Analog Voice Ports

Overview

Connecting voice devices to a network infrastructure requires an in-depth understanding of the signaling and electrical characteristics that are specific to each type of interface. Improperly matched electrical components can cause echo and create poor audio quality. Configuring devices for international implementation requires knowledge of country-specific settings. This lesson examines analog voice ports, analog signaling, and configuration parameters for analog voice ports.

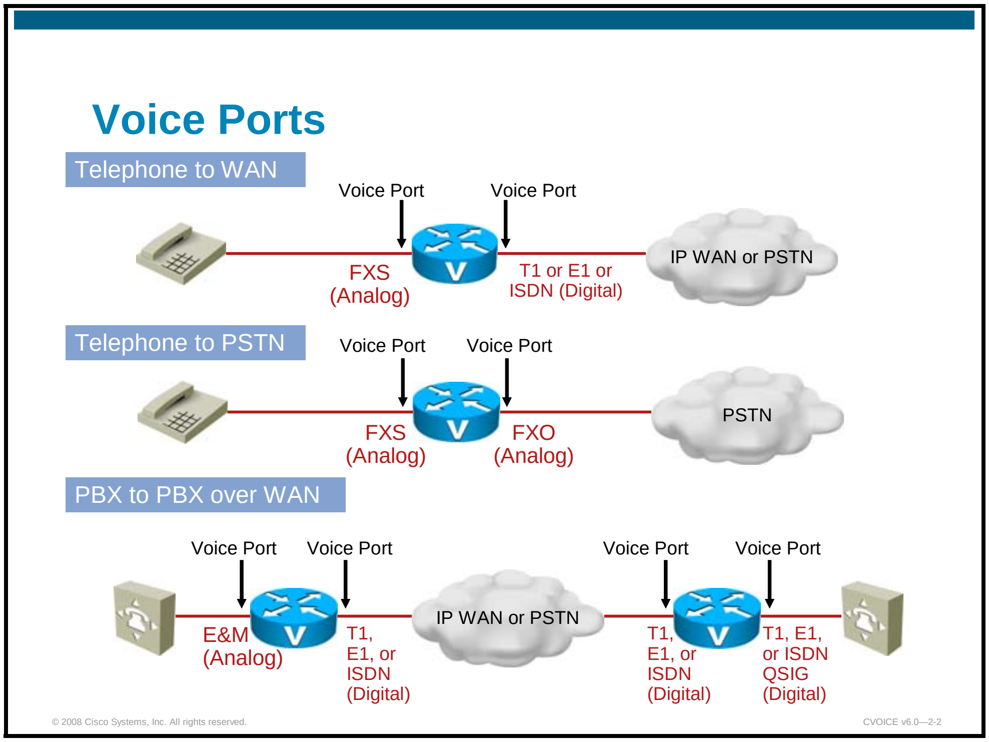
Objectives

Upon completing this lesson, you will be able to describe the various analog voice interfaces and how to configure them. This ability includes being able to meet these objectives:

- Describe the various types of voice port interfaces and where they are used
- Describe the various types of analog interfaces and their characteristics
- Describe how to configure three types of analog voice ports
- Describe CAMA and how to configure a voice port for CAMA
- Describe how to configure voice ports for DID service
- Describe timing configuration parameters on voice ports
- Explain how to use **show**, **test**, and **debug** commands to verify analog voice port operation

Voice Ports

This topic describes the various types of voice ports and where they are used.



Voice Ports

Telephone to WAN

Voice Port

Voice Port

FXS (Analog)

T1 or E1 or ISDN (Digital)

IP WAN or PSTN

Telephone to PSTN

Voice Port

Voice Port

FXS (Analog)

FXO (Analog)

PSTN

PBX to PBX over WAN

Voice Port

Voice Port

E&M (Analog)

T1, E1, or ISDN (Digital)

IP WAN or PSTN

Voice Port

Voice Port

T1, E1, or ISDN (Digital)

T1, E1, or ISDN QSIG (Digital)

CVOICE v6.0—2-2

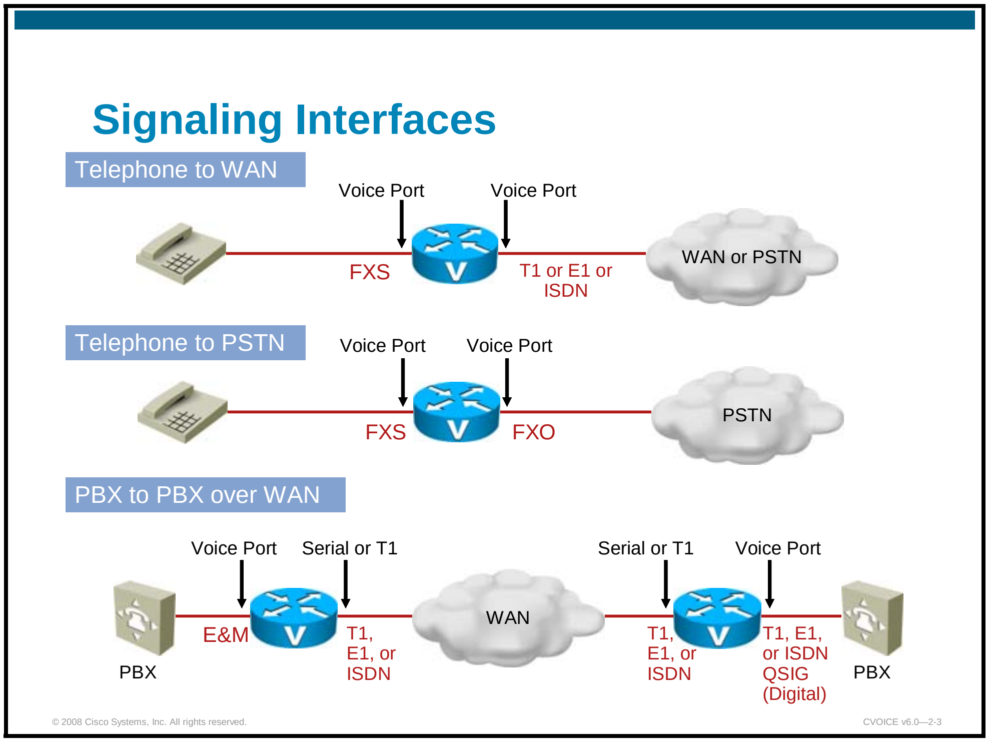
Voice ports on routers and access servers emulate physical telephony switch connections so that voice calls and their associated signaling can be transferred intact between a packet network and a circuit-switched network or device. For a voice call to occur, certain information, such as the on-hook status of telephony devices, the availability of the line, and whether an incoming call is trying to reach a device, must be passed between the telephony devices at either end of the call. This information is referred to as signaling, and to process it properly, the devices at both ends of the call segment, which are directly connected to each other, must use the same type of signaling.

The devices in the packet network must be configured to convey signaling information in a way that the circuit-switched network can understand. They must also be able to understand signaling information that is received from the circuit-switched network. Circuit-switched signaling is accomplished by installing appropriate voice hardware in the router or access server and by configuring the voice ports that connect to telephony devices or the circuit-switched network.

The figure shows typical examples of how voice ports are used.

Signaling Interfaces

This subtopic covers various signaling interfaces.



Voice ports on routers and access servers physically connect the router, access server or call control device to telephony devices such as telephones, fax machines, PBXs, and PSTN central office (CO) switches through signaling interfaces. The figure shows how the different signaling interfaces are associated with different uses of voice ports.

These signaling interfaces generate information about things such as the following:

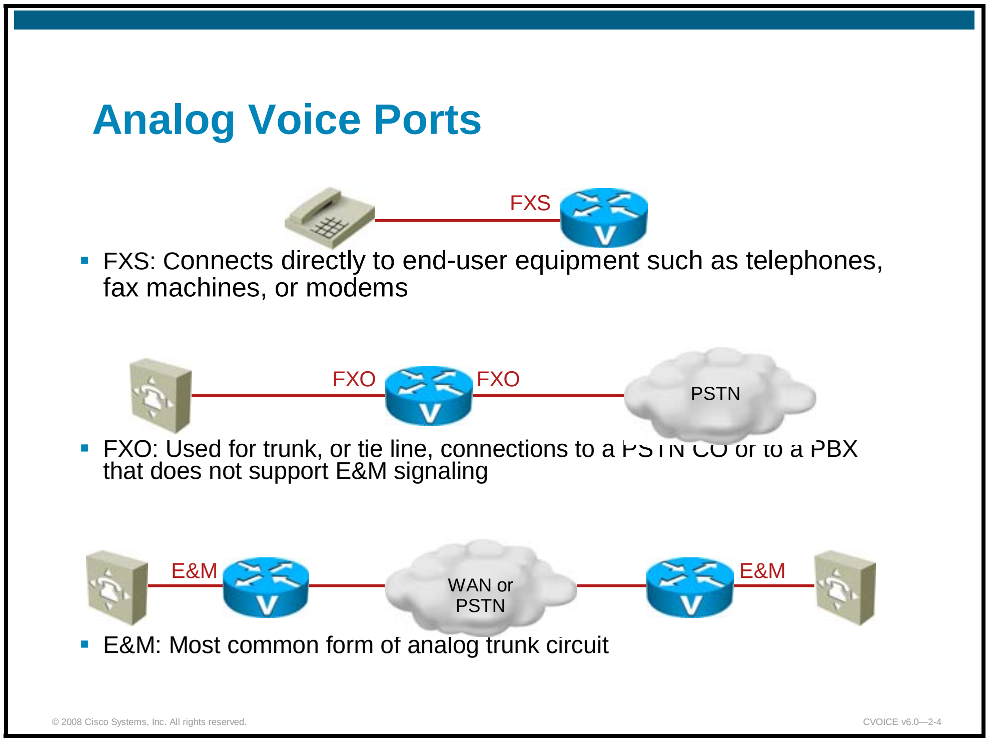
- On-hook status
- Ringing
- Line seizure

The voice port hardware and software of the router need to be configured to transmit and receive the same type of signaling being used by the device with which they are interfacing so that calls can be exchanged smoothly between the packet network and the circuit-switched network.

The signaling interfaces discussed in the next sections include Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), and recEive and transMit (E&M), which are types of analog interfaces. Digital signaling interfaces include T1, E1, and ISDN. Some digital connections emulate FXO, FXS, and E&M interfaces. It is important to know which signaling method the telephony side of the connection is using, and to match the router configuration and voice interface hardware to that signaling method.

Analog Voice Ports

This topic describes the various types of analog interfaces and their characteristics.



Analog Voice Ports

- FXS: Connects directly to end-user equipment such as telephones, fax machines, or modems
- FXO: Used for trunk, or tie line, connections to a PSTN CO or to a PBX that does not support E&M signaling
- E&M: Most common form of analog trunk circuit

CVOICE v6.0—2-4

Analog voice port interfaces connect routers in packet-based networks to analog two-wire or four-wire analog circuits in telephony networks. Two-wire circuits connect to analog telephone or fax devices, and four-wire circuits connect to PBXs. Connections to the PSTN CO are typically made with digital interfaces. There are three types of analog voice interfaces that Cisco gateways support.

FXS Interfaces

An FXS interface connects the router or access server to end-user equipment such as telephones, fax machines, or modems. The FXS interface supplies ring, voltage, and dial tone to the station and includes an RJ-11 connector for basic telephone equipment, key sets, and PBXs.

FXO Interfaces

An FXO interface is used for trunk, or tie-line, connections to a PSTN CO or to a PBX that does not support E&M signaling (when local telecommunications authority permits). This interface is of value for off-premises station applications. A standard RJ-11 modular telephone cable connects the FXO voice interface card to the PSTN or PBX through a telephone wall outlet.

E&M Interfaces

Trunk circuits connect telephone switches to one another; they do not connect end-user equipment to the network. The most common form of analog trunk circuit is the E&M interface, which uses special signaling paths that are separate from the trunk audio path to convey information about the calls. The signaling paths are known as the E-lead and the M-lead. E&M connections from routers to telephone switches or to PBXs are preferable to FXS and FXO connections because E&M provides better answer and disconnect supervision.

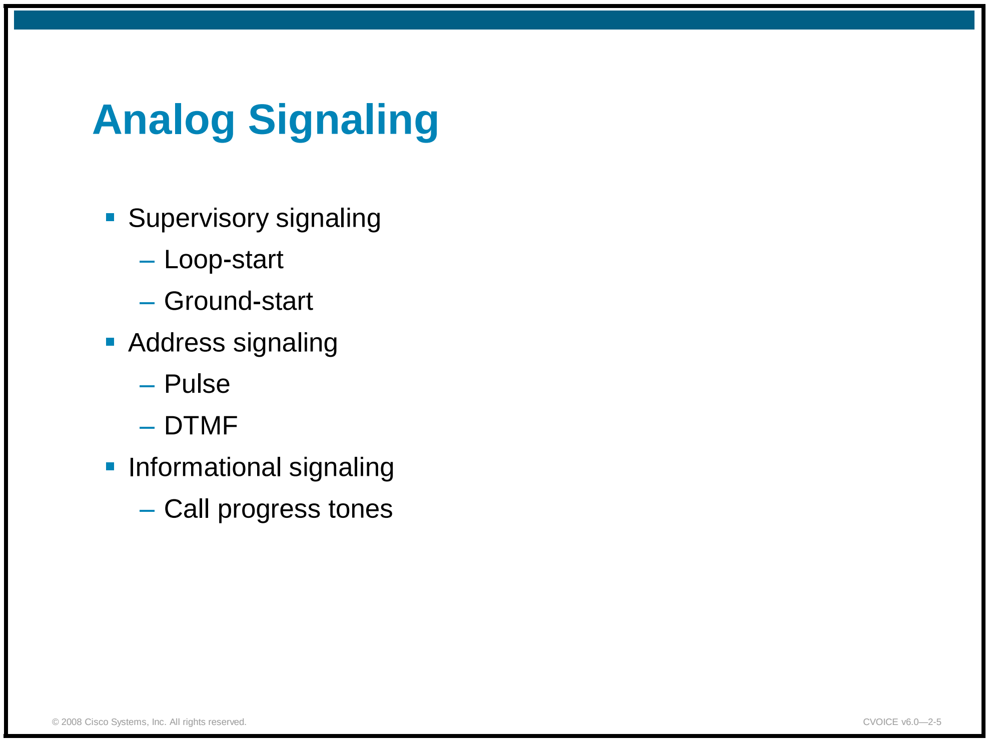
The name E&M is thought to derive from the phrase “ear and mouth” or “recEive and transMit,” although it could also have come from “Earth and Magneto.” The history of these names dates back to the early days of telephony, when the CO side had a key that grounded the E circuit, and the other side had a sounder with an electromagnet attached to a battery. Descriptions such as ear and mouth were adopted to help field personnel understand and determine the direction of a signal in a wire.

Like a serial port, an E&M interface has a DTE or DCE type of reference. In the telecommunications world, the trunking side is similar to the DCE and is usually associated with CO functionality. The router acts as this side of the interface. The other side is referred to as the signaling side, like a DTE, and is usually a device such as a PBX.

Note Depending on how the router is connected to the PSTN, the voice gateway may provide a clock signal to an attached key system or PBX because the PSTN has more accurate clocks, and the voice gateway can pass this capability to downstream devices.

Analog Signaling

This subtopic covers analog signaling.



Analog Signaling

- Supervisory signaling
  - Loop-start
  - Ground-start
- Address signaling
  - Pulse
  - DTMF
- Informational signaling
  - Call progress tones

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-5

The human voice generates sound waves, and the telephone converts the sound waves into electrical signals, analogous to sound. Analog signaling is not robust because of line noise. Analog transmissions are boosted by amplifiers because the signal diminishes the farther it travels from the CO. As the signal is boosted, the noise is also boosted, which often causes an unusable connection.

In digital networks, signals are transmitted over great distances and coded, regenerated, and decoded without degradation of quality. Repeaters amplify the signal and clean it to its original condition. Repeaters then determine the original sequence of the signal levels and send the clean signal to the next network destination.

Voice ports on routers and access servers physically connect the router or access server to telephony devices such as telephones, fax machines, PBXs, and PSTN CO switches. These devices may use any of several types of signaling interfaces to generate information about on-hook status, ringing, and line seizure.

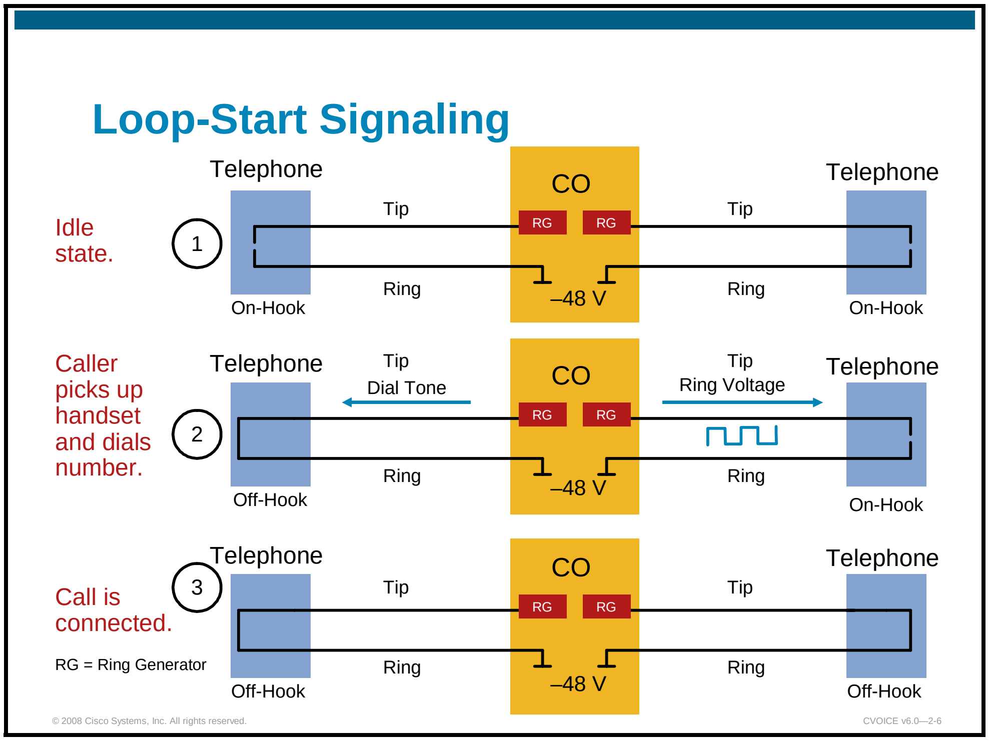
Signaling techniques can be placed into one of three categories:

- **Supervisory:** Involves the detection of changes to the status of a loop or trunk. Once these changes are detected, the supervisory circuit generates a predetermined response. A circuit (loop) can close to connect a call, for example.
- **Addressing:** Involves passing dialed digits (pulsed or tone) to a PBX or CO. These dialed digits provide the switch with a connection path to another phone or customer premises equipment (CPE).
- **Informational:** Provides audible tones, which indicate certain conditions such as an incoming call or a busy phone, to the user.

Note A phone call cannot take place without these signaling techniques.

FXS and FXO Supervisory Signaling

This subtopic covers FXS and FXO supervisory signaling.



XO and FXS interfaces indicate on-hook or off-hook status and the seizure of telephone lines by one of two access signaling methods: loop-start or ground-start. The type of access signaling is determined by the type of service from the CO; standard home telephone lines use loop-start, but business telephones can order ground-start lines instead.

Loop-start is the more common access signaling technique. When a handset is picked up (the telephone goes off hook), the 48-V circuit becomes closed, which draws current from the telephone company CO and indicates a change in status. This change in status signals the CO to provide a dial tone. The CO signals an incoming call to the called handset by using a “Ring Generator” (RG) to send a signal in a standard on/off pattern, which causes the telephone to ring. When the called subscriber answers the call, the 48-V circuit is closed and the CO turns off the ring voltage. At this point, the two circuits are tied together at the CO.

Loop-Start Signaling Process

The loop-start signaling process is as follows:

1. In the idle state, the telephone, PBX, or FXO module has an open two-wire loop (the tip and ring lines are open). The loop could be a telephone set with the handset on-hook, or a PBX or FXO module that generates an open loop between the tip and ring lines. The CO or FXS waits for a closed loop that generates a current flow. The CO or FXS has a ring generator connected to the tip line and –48 VDC on the ring line.

2. A telephone set, PBX, or FXO module closes the loop between the tip and ring lines. The telephone handset goes off hook or the PBX or FXO module closes a circuit connection. The CO or FXS module detects current flow and then generates a dial tone, which is sent to the telephone set, PBX, or FXO module. The dial tone indicates that the customer can start to dial. At the same time, the CO or FXS module seizes the ring line of the called telephone, PBX, or FXO module by superimposing a 20-Hz, 90-VAC signal over the –48VDC ring line. This procedure rings the called party telephone set or signals the PBX or FXS module that there is an incoming call. The CO or FXS module removes this ring once the telephone set, PBX, or FXO module closes the circuit between the tip and ring lines.
3. The telephone set closes the circuit when the called party picks up the handset. The PBX or FXS module closes the circuit when it has an available resource to connect to the called party.

Disadvantages

Loop-start has two disadvantages:

- There is no way to prevent the CO and the subscriber from seizing the same line at the same time, a condition known as "glare."

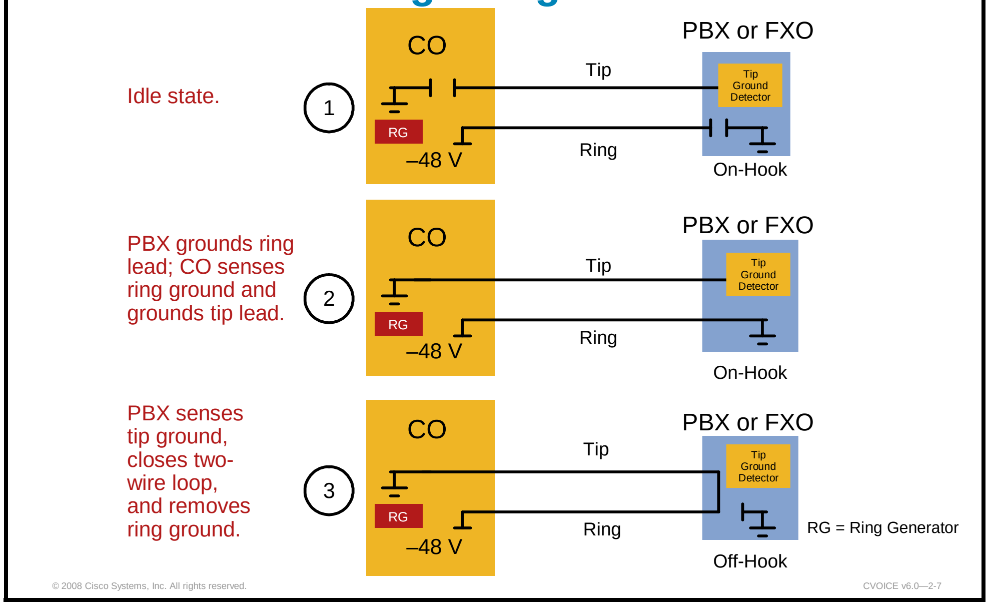
  It takes about four seconds for the CO switch to cycle through all the lines it must ring. This delay in ringing a phone causes glare as the CO switch and the telephone set seize a line simultaneously. When this happens, the person who initiated the call is connected to the called party almost instantaneously, with no ringback tone.

Tip The best way to prevent glare is to use ground-start signaling.

- It does not provide switch-side disconnect supervision for FXO calls. The telephony switch is the connection in the PSTN, another PBX, or key system. This switch expects the FXO interface of the router, which looks like a telephone to the switch, to hang up the calls that it receives through its FXO port. However, this function is not built into the router for received calls. It only operates for calls originating from the FXO port.

These disadvantages are usually not a problem on residential telephones, but they become significant with the higher call volume that is experienced on business telephones.

Ground-Start Signaling



CVOICE v6.0—2-7

Ground-start signaling is another supervisory signaling technique, like loop-start, that provides a way to indicate on-hook and off-hook conditions in a voice network. Ground-start signaling is used primarily in switch-to-switch connections. The main difference between ground-start and loop-start signaling is that ground-start requires ground detection to occur in both ends of a connection before the tip and ring loop can be closed.

Ground-start signaling works by using ground and current detectors that allow the network to indicate off-hook or seizure of an incoming call independent of the ringing signal and allow for positive recognition of connects and disconnects. Because ground-start signaling uses a request or confirm switch, or both, at both ends of the interface, it is preferable over FXOs and other signaling methods on high-usage trunks. For this reason, ground-start signaling is typically used on trunk lines between PBXs and in businesses where call volume on loop-start lines can result in glare.

Ground-Start Signaling Process

The ground-start signaling process is as follows:

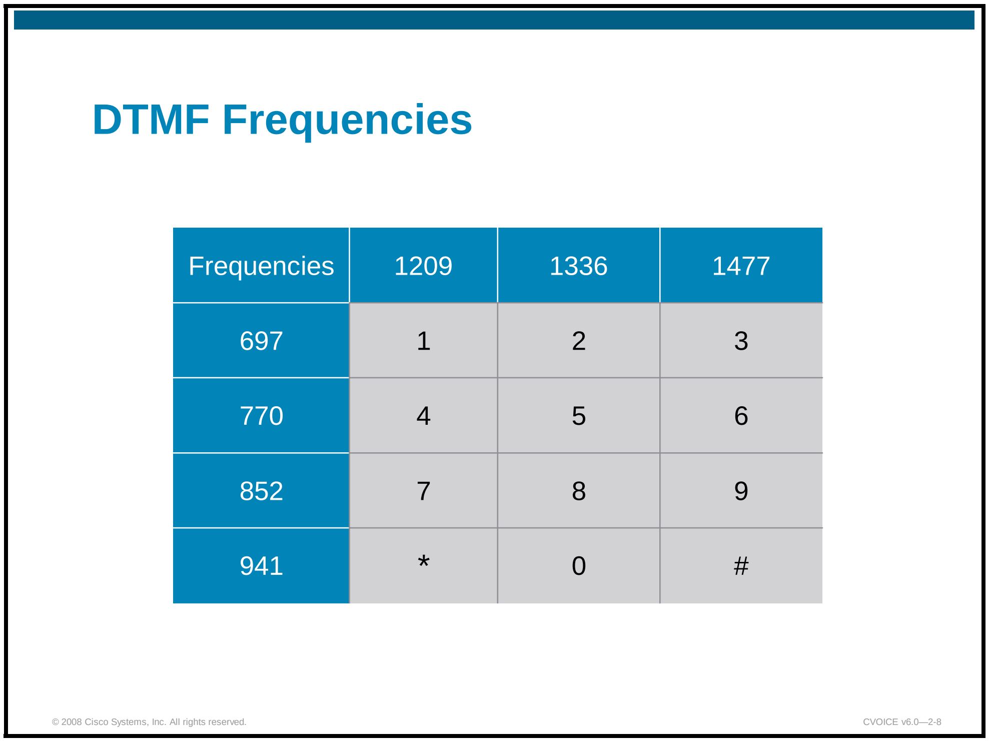
1. In the idle state, both the tip and ring lines are disconnected from ground. The PBX and FXO constantly monitor the tip line for ground, and the CO and FXS constantly monitor the ring line for ground. Battery (–48 VDC) is still connected to the ring line just as in loop-start signaling.

2. A PBX or FXO grounds the ring line to indicate to the CO or FXS that there is an incoming call. The CO or FXS senses the ring ground and then grounds the tip lead to let the PBX or FXO know that it is ready to receive the incoming call.

3. The PBX or FXO senses the tip ground and closes the loop between the tip and ring lines in response. It also removes the ring ground.

Analog Address Signaling

This subtopic covers analog address signaling.



DTMF Frequencies

Frequencies	1209	1336	1477
697	1	2	3
770	4	5	6
852	7	8	9
941	*	0	#

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-8

The dialing phase allows the subscriber to enter a phone number (address) of a telephone at another location. The customer enters this number with either a rotary phone that generates pulses or a touch-tone (push-button) phone that generates tones.

Telephones use two different types of address signaling to notify the telephone company where a subscriber is calling:

- Pulse dialing
- DTMF dialing

These pulses or tones are transmitted to the CO switch across a two-wire twisted-pair cable (tip and ring lines). On the voice gateway, the FXO port sends address signaling to the FXS port. This address indicates the final destination of the call.

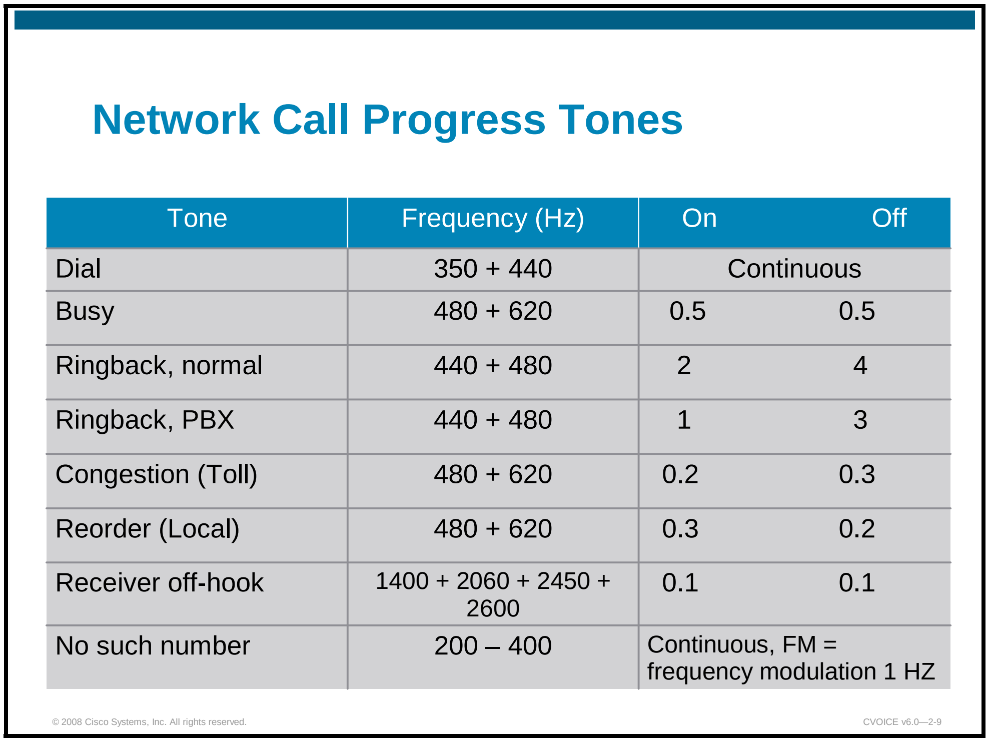
Pulsed tones were used by the old rotary phones. These phones had a disk that rotated to dial a number. As the disk rotated, it opened and closed the circuit a specified number of times based on how far the disk was turned. The exchange equipment counted those circuit interruptions to determine the called number. The duration of open-to-closed times had to be within specifications according to the country you were in.

Now, analog circuits use DTMF tones to indicate the destination address. DTMF assigns a specific frequency (consisting of two separate tones) to each key on the touch-tone telephone dial pad. The combination of these two tones notifies the receiving subscriber of the digits dialed.

The table in the figure shows the frequency tones that are generated by dual tone multifrequency (DTMF) dialing.

Informational Signaling

This subtopic covers informational signaling.



Network Call Progress Tones

Tone	Frequency (Hz)	On	Off
Dial	350 + 440	Continuous	
Busy	480 + 620	0.5	0.5
Ringback, normal	440 + 480	2	4
Ringback, PBX	440 + 480	1	3
Congestion (Toll)	480 + 620	0.2	0.3
Reorder (Local)	480 + 620	0.3	0.2
Receiver off-hook	1400 + 2060 + 2450 + 2600	0.1	0.1
No such number	200 – 400	Continuous, FM = frequency modulation 1 HZ	

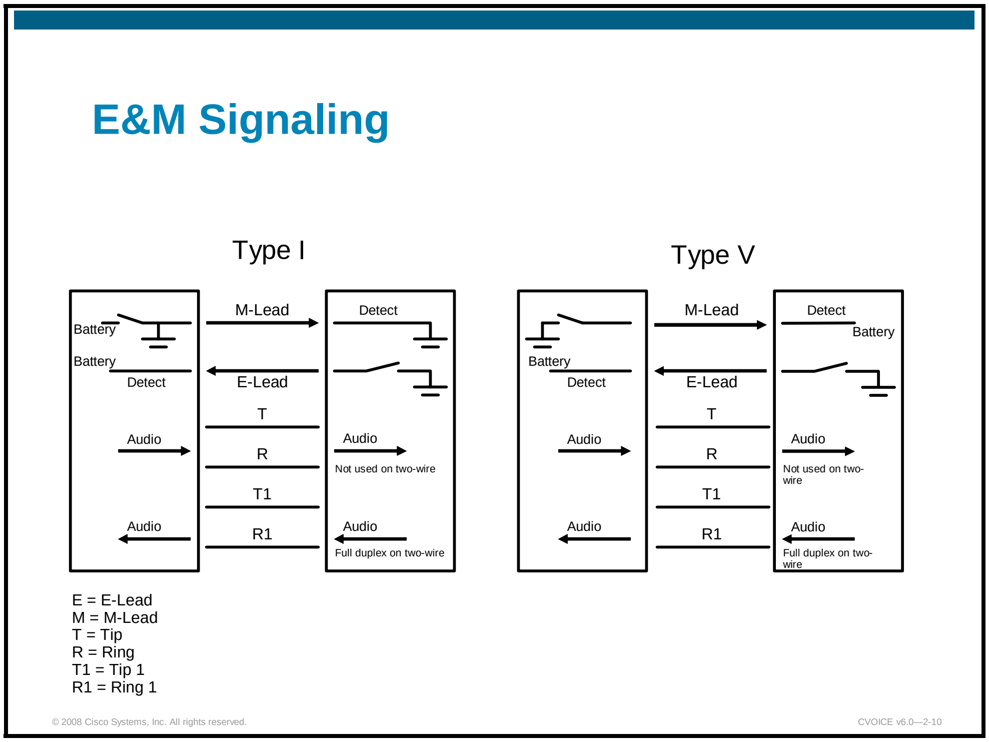
CVOICE v6.0—2-9

The FXS port provides informational signaling using call progress (CP) tones. These CP tones are audible and are used by the FXS-connected device to indicate the status of calls. The progress tones listed in the table above are for North American phone systems. International phone systems can have a totally different set of progress tones. All network administrators must be familiar with most of these CP tones:

- **Dial tone:** Indicates that the telephone company is ready to receive digits from the user telephone
- **Busy tone:** Indicates that a call cannot be completed because the telephone at the remote end is already in use
- **Ringback (normal or PBX) tone:** Indicates that the telephone company is attempting to complete a call on behalf of a subscriber
- **Congestion progress tone:** Is used between switches to indicate that congestion in the long-distance telephone network currently prevents a telephone call from being progressed
- **Reorder tone:** Indicates that all the local telephone circuits are busy, and thus prevents a telephone call from being processed
- **Receiver off-hook tone:** Is the loud ringing that indicates the receiver of a phone is left off hook for an extended period of time
- **No such number tone:** Indicates that the number dialed cannot be found in the routing table of a switch

E&M Signaling

This subtopic covers E&M signaling.



E&M Signaling

E = E-Lead
M = M-Lead
T = Tip
R = Ring
T1 = Tip 1
R1 = Ring 1

E&M is another signaling technique used mainly between PBXs or other network-to-network telephony switches (such as the Lucent 5 Electronic Switching System [5ESS] and Nortel DMS-100). 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.

There are six distinct physical configurations for the signaling part of the interface; they are Types I to V and Signaling System Direct Current No. 5 (SSDC5). They use different methods to signal on-hook or off-hook status, as shown in the following table. Cisco voice implementation supports E&M Types I, II, III, and V.

E&M Signaling Types

Type	M-Lead Off-Hook	M-Lead On-Hook	E-Lead Off-Hook	E-Lead On-Hook
I	Battery	Ground	Ground	Open
II	Battery	Open	Ground	Open
III	Loop current	Ground	Ground	Open
IV	Ground	Open	Ground	Open
V	Ground	Open	Ground	Open
SSDC5	Earth on	Earth off	Earth on	Earth off

Type I

Type I signaling is the most common E&M signaling method used in North America. One wire is the E-lead, another 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 M- and E-leads. In the idle (on-hook) state, both the E- and M-lead are open as in the diagram above. The PBX indicates an off-hook by connecting the M-lead to the battery. The line side indicates an off-hook by connecting the E-lead to ground.

Type II

Type II signaling is typically used in sensitive environments because it produces very little interference. This type uses four wires for signaling. One wire is the E-lead, another wire is the M-lead, and the 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 PBX side indicates an off-hook by connecting the M-lead to the SB lead. The line side indicates an off-hook by connecting the E-lead to SG lead.

Type III

Type III signaling is not commonly used. Type III also uses four wires for signaling. In the idle state (on-hook), the E-lead is open and the M-lead is connected to the SG lead, which is grounded. The PBX side indicates an off-hook by moving the M-lead from the SG lead to the SB lead. The line side indicates an off-hook by grounding the E-lead.

Type IV

Type IV also uses four wires for signaling. In the idle state (on-hook), the E- and M-leads are both open. The PBX side indicates an off-hook by connecting the M-lead to the SB lead, which is grounded on the line side. The line side indicates an off-hook by connecting the E-lead to the SG lead, which is grounded on the PBX side.

Note E&M Type IV is not supported. However, the way Type IV operates is similar to Type II, except for the M-lead operation. On Type IV, the M-lead states are open/ground, whereas the Type II M-lead states are open and battery. Type IV can interface with Type II. To use Type IV, you can set the E&M voice port to Type II and perform the necessary M-lead rewiring.

Type V

Type V is the most common E&M signaling form used outside of North America. Type V is similar to Type I because two wires are used for signaling (one wire is the E-lead and the other wire is the M-lead). In the idle (on-hook) state, both the E- and M-lead are open as in the diagram above. The PBX indicates an off-hook by grounding the M-lead. The line side indicates an off-hook by grounding the E-lead.

SSDC5

Although SSDC5 is similar to Type V, SSDC5 differs in that on- and off-hook states are backward to allow for fail-safe operation. If the line breaks, the interface defaults to off-hook (busy). SSDC5 is most often found in England.

Physical Interface

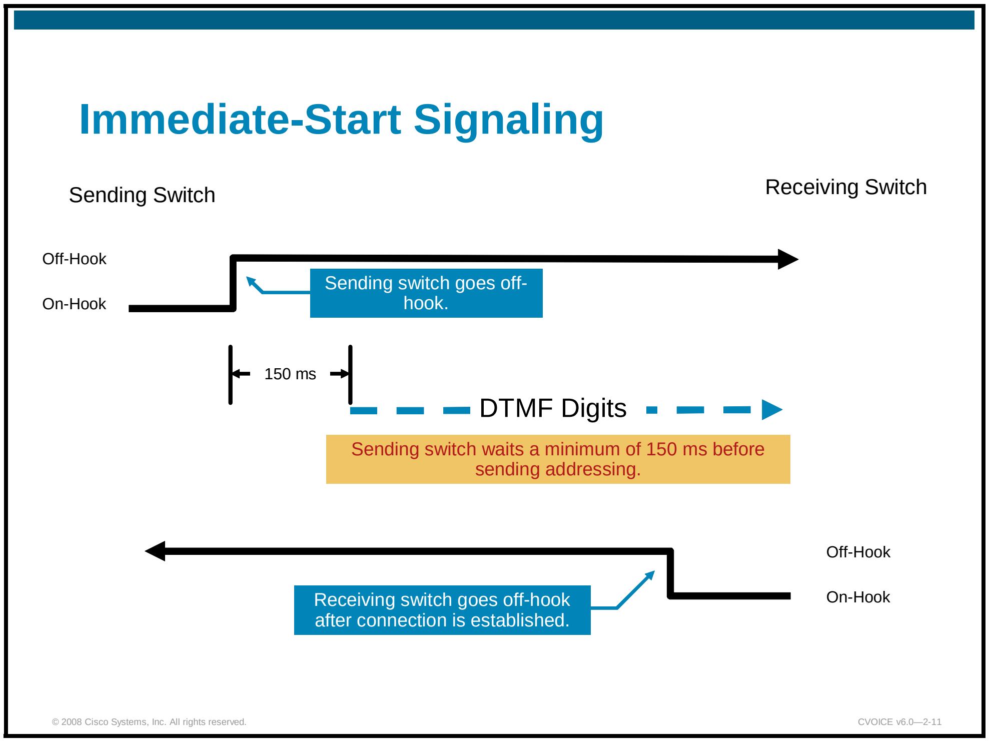
The physical E&M interface is an RJ-48 connector that connects to PBX trunk lines, which are classified as either two-wire or four-wire.

Note Two-wire and four-wire refer to the voice wires. A connection may be called a four-wire E&M circuit although it actually has six to eight physical wires.

Two or four wires are used for signaling and the remaining two pairs of wires serve as the audio path. This refers to whether the audio path is full duplex on one pair of wires (two-wire) or on two pair of wires (four-wire).

E&M Address Signaling

This subtopic covers E&M address signaling.



Immediate-Start Signaling

Sending Switch

Receiving Switch

Off-Hook

On-Hook

Sending switch goes off-hook.

150 ms

DTMF Digits

Sending switch waits a minimum of 150 ms before sending addressing.

Off-Hook

On-Hook

Receiving switch goes off-hook after connection is established.

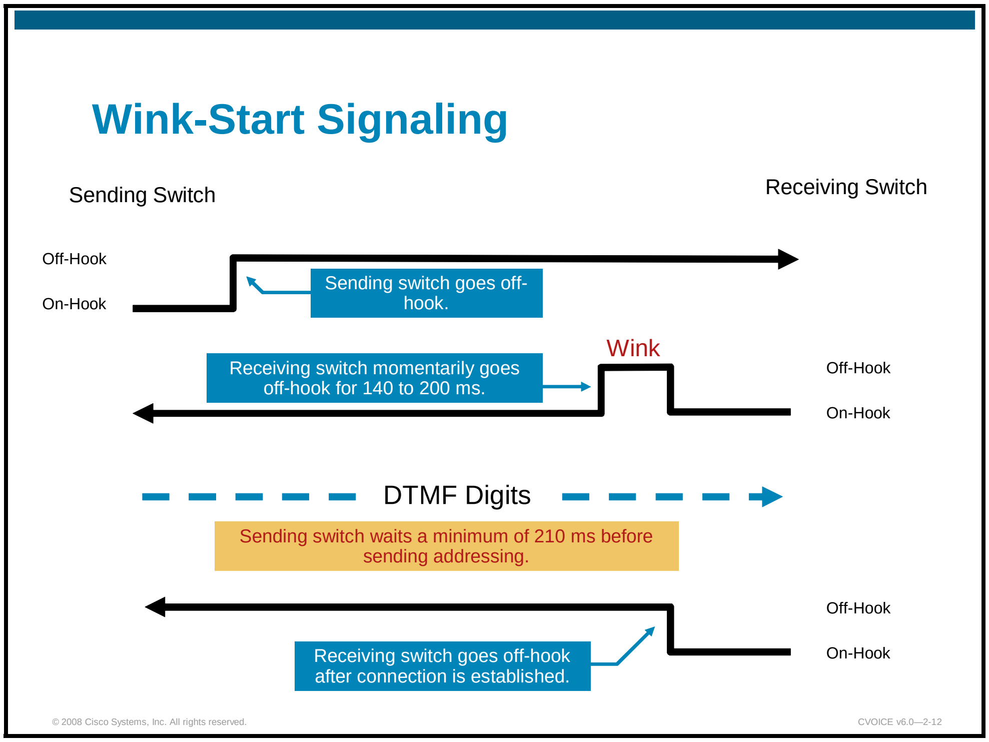
CVOICE v6.0—2-11

PBXs built by different manufacturers can indicate on-hook or off-hook status and telephone line seizure on the E&M interface by using any of three types of access signaling:

- **Immediate-start signaling**
- **Wink-start signaling**
- **Delay-start signaling**

Immediate-start Signaling

Immediate-start signaling is the simplest method of E&M access signaling. The calling side seizes the line by going off hook on its E-lead, waits for a minimum of 150 ms, and then sends address information as DTMF digits or as dialed pulses. This type of signaling is used for E&M tie trunk interfaces. The slide above represents immediate-start signaling.



Wink-Start Signaling

Sending Switch

Receiving Switch

Off-Hook

On-Hook

Sending switch goes off-hook.

Wink

Receiving switch momentarily goes off-hook for 140 to 200 ms.

Off-Hook

On-Hook

DTMF Digits

Sending switch waits a minimum of 210 ms before sending addressing.

Receiving switch goes off-hook after connection is established.

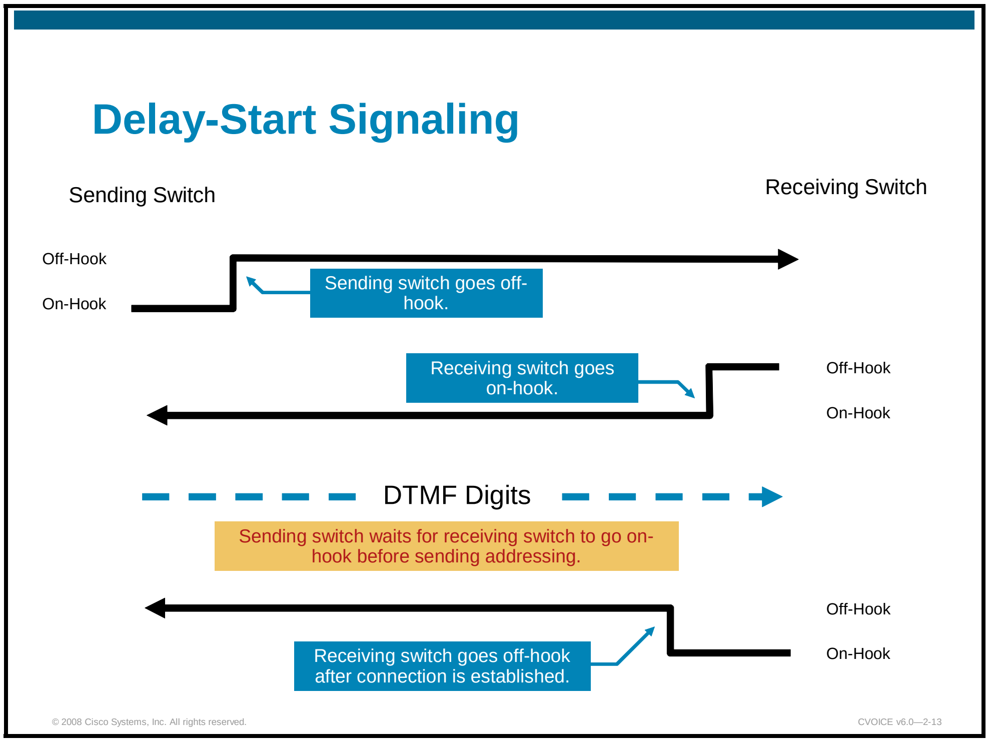
Off-Hook

On-Hook

The figure above shows the wink-start signaling process.

Wink-start Signaling

Wink-start signaling is the most commonly used method for E&M access signaling and the default for E&M voice ports. Wink-start was developed to minimize glare, a condition found in immediate-start E&M, in which both ends attempt to seize a trunk at the same time. In wink-start, the calling side seizes the line by going off hook on its E-lead, and then waits for a short, temporary off-hook pulse, or “wink,” from the other end on its M-lead before sending address information as DTMF digits. The switch interprets the pulse as an indication to proceed and then sends the dialed digits as DTMF or dialed pulses. This type of signaling is used for E&M tie trunk interfaces. It is the default setting for E&M voice ports.



Delay-Start Signaling

Sending switch goes off-hook.

Receiving switch goes on-hook.

Sending switch waits for receiving switch to go on-hook before sending addressing.

Receiving switch goes off-hook after connection is established.

CVOICE v6.0—2-13

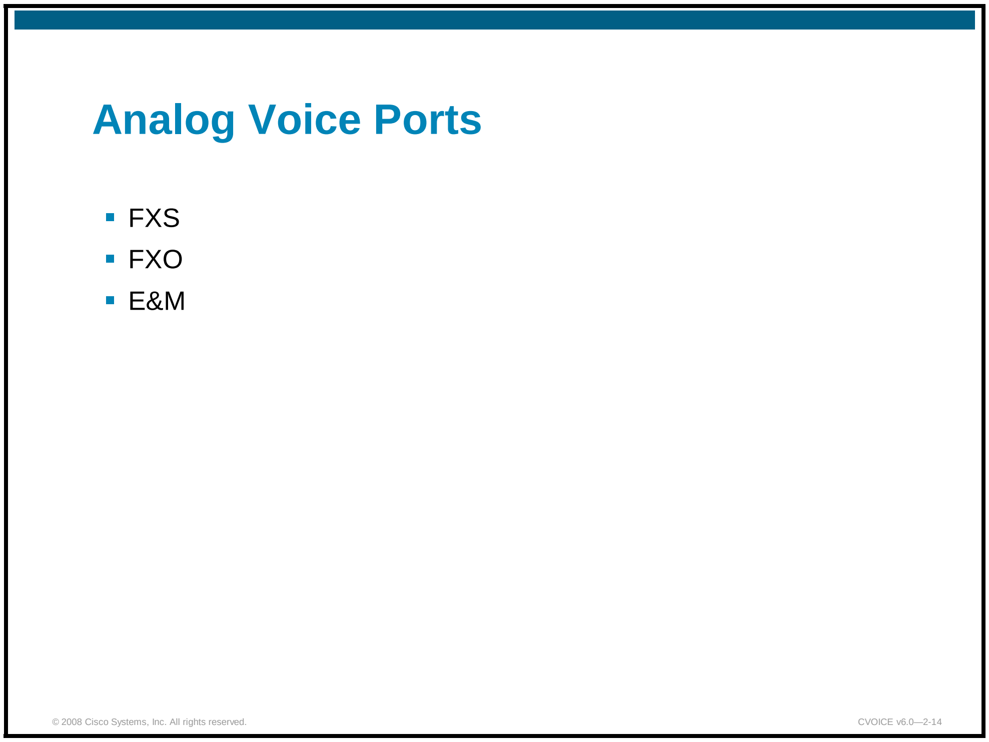
The figure above shows the delay-start signaling process.

Delay-start Signaling

The calling station seizes the line by going off hook on its E-lead. After a timed interval, the calling side looks at the status of the called side. If the called side is on-hook, the calling side starts sending information as DTMF digits; otherwise, the calling side waits until the called side goes on-hook and then starts sending address information. This type of signaling is used for E&M tie trunk interfaces.

Configuring Analog Voice Ports

This topic describes how to configure the three types of analog voice ports.



Analog Voice Ports

- FXS
- FXO
- E&M

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—2-14

These are the three types of analog ports that you will learn to configure:

- FXS
- FXO
- E&M

The following subtopics describe how to configure analog voice ports.

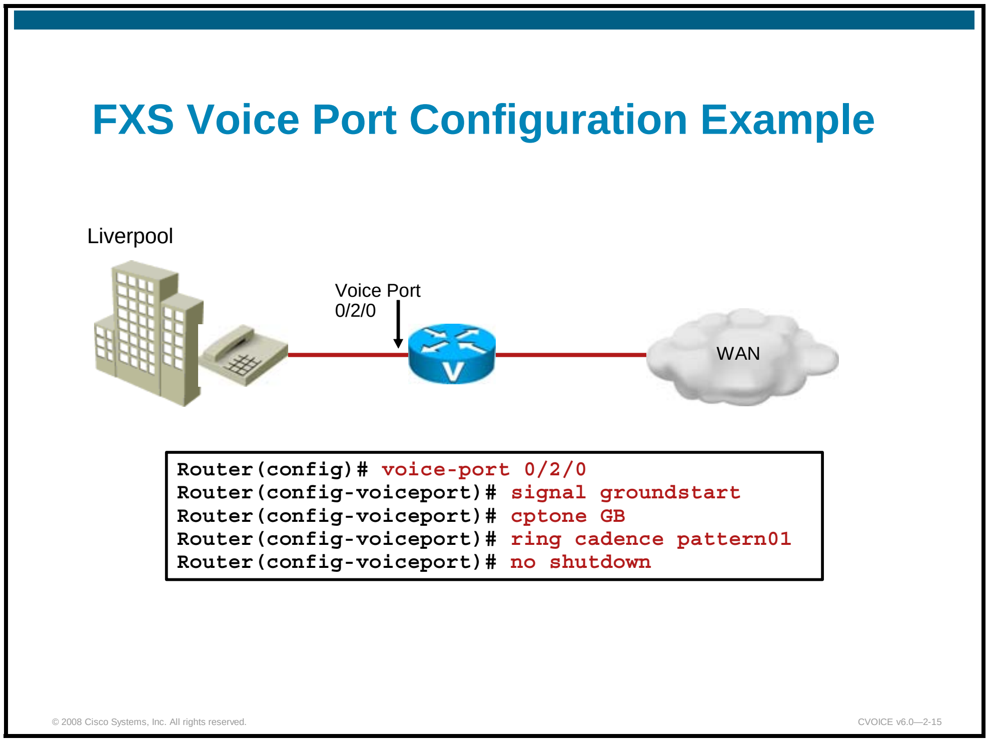
In North America, the FXS port connection functions with default settings most of the time. The same cannot be said for other countries and continents. Remember, FXS ports look like switches to the edge devices that are connected to them. Therefore, the configuration of the FXS port should emulate the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

When to Configure an FXS Port

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

FXS Voice Port Configuration Example

This subtopic shows an FXS voice port configuration example.



FXS Voice Port Configuration Example

```
Router(config)# voice-port 0/2/0
Router(config-voiceport)# signal groundstart
Router(config-voiceport)# cptone GB
Router(config-voiceport)# ring cadence pattern01
Router(config-voiceport)# no shutdown
```

CVOICE v6.0—2-15

In this example, you have been assigned to configure a voice gateway to route calls to a plain old telephone service (POTS) phone connected to a FXS port on a remote router in Great Britain. The diagram above shows how the British office is configured to enable ground-start signaling on FXS voice port 0/2/0. The call-progress tones are set for Great Britain, and the ring cadence is set for pattern 1.

The requirements are as follows:

- Configure the voice port to use ground-start signaling
- Configure the CP tones for Great Britain

Complete these steps to configure a FXS voice port.

Step 1 Enter voice-port configuration mode.

```
Router(config# voice-port slot/port
```

Step 2 Select the access signaling type to match that of the telephony connection that you are making.

```
Router(config-voiceport)# signal {loopstart | groundstart}
```

Caution If you change signal type, you must execute a **shutdown** and **no shutdown** on the voice port.

Step 3 Select the two-letter locale for the voice CP tones and other locale-specific parameters to be used on this voice port.

```
Router(config-voiceport)# cptone locale
```

Step 4 Specify a ring pattern. Each pattern specifies a ring pulse time and a ring interval time.

```
Router(config-voiceport)# ring cadence {pattern-number |
define pulse interval}
```

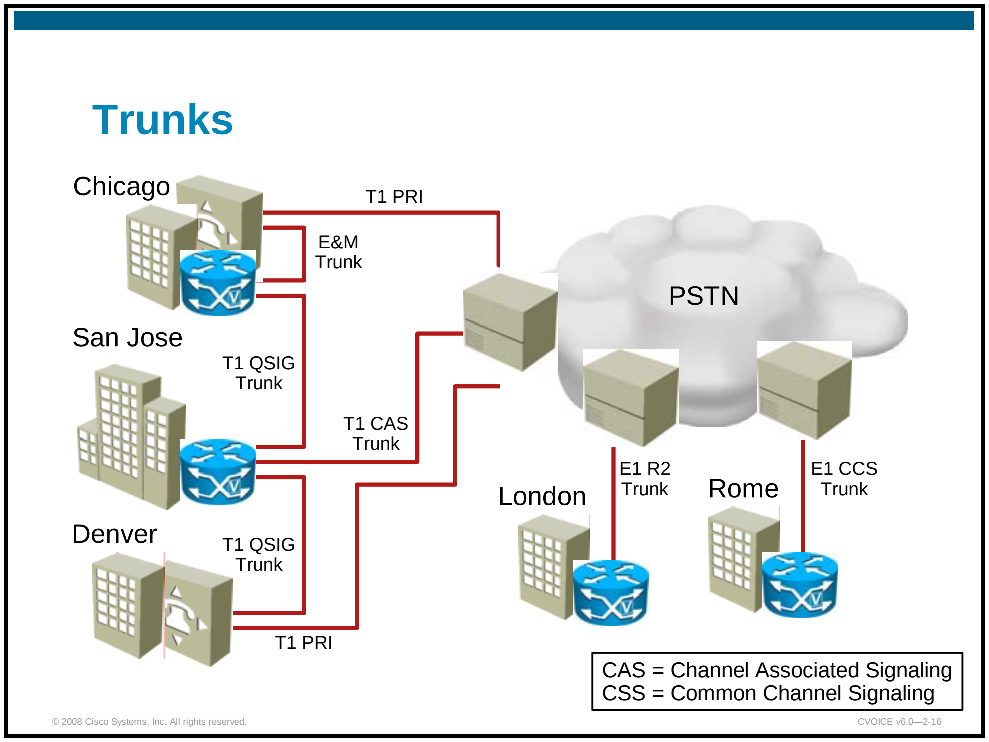
The **patternXX** keyword provides preset ring cadence patterns for use on any platform. The **define** keyword allows you to create a custom ring cadence. On the router, only one or two pairs of digits can be entered under the **define** keyword.

Step 5 Activate the voice port.

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

Trunks

This subtopic describes trunks and associated signaling.



Trunks

CAS = Channel Associated Signaling
CSS = Common Channel Signaling

Trunks are used to interconnect gateways or PBX systems to other gateways, PBX systems, or the PSTN. A trunk is a single physical or logical interface that contains several physical interfaces and connects to a single destination. This destination could be a single FXO port that provides a single line connection between a Cisco gateway and an FXS port of small PBX system, a POTS device, or several T1 interfaces, with 24 lines each in a Cisco gateway, that provide PSTN lines to several hundred subscribers.

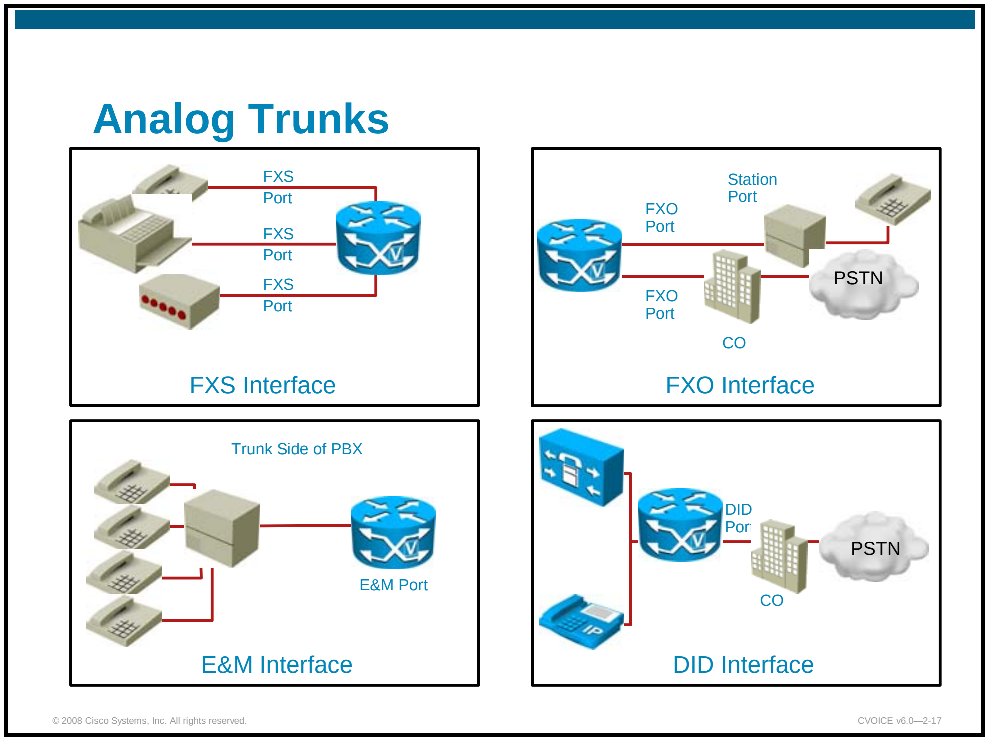
Trunk ports can be analog or digital and use a variety of signaling protocols. Signaling can be done using either the voice channel (in-band) or an extra dedicated channel (out-of-band). The available features depend on the signaling protocol in use between the devices.

The diagram in the figure illustrates a variety of possible trunk connections:

- If a subscriber at the London site places a call to the PSTN, the gateway uses one voice channel of the E1 R2 trunk interface.
- If a subscriber of the legacy PBX system at the Chicago site needs to place a call to a subscriber with an IP phone that is connected to the Chicago gateway, the call will route via one channel of the E&M trunk between the legacy PBX and the gateway.
- The Denver and the Chicago sites are connected to San Jose via Q Signaling (QSIG) to build up a common private numbering plan between those sites. Because the Cisco IP telephony rollout in Denver has not started yet, the QSIG trunk is established directly between the San Jose gateway and the Denver legacy PBX.

Analog Trunks

This subtopic covers analog trunks. Digital trunks are covered in the “Understanding Digital Voice Ports” lesson.



Analog Trunks

FXS Interface

FXO Interface

E&M Interface

DID Interface

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-17

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

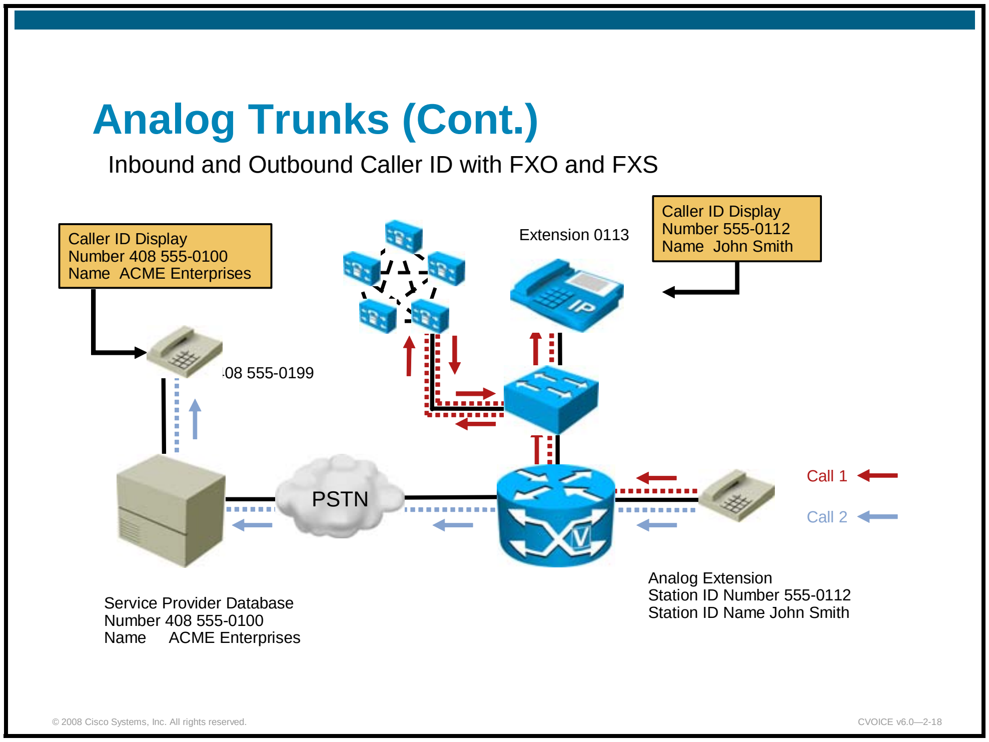
To implement a Cisco voice gateway into an analog trunk environment, the FXS, FXO, direct inward dialing (DID), and E&M interfaces are commonly used.

PSTN carriers typically offer analog trunk features that can be supported on home phones. The following table presents a description of the common analog trunk features.

Analog Trunk Features

Feature	Description
Caller ID	Caller ID allows users to see the calling number before answering the phone.
Message waiting light	There are two methods used to activate the analog message waiting light: ■ High DC voltage Message Waiting Indicator (MWI) light and frequency-shift keying (FSK) messaging ■ Stuttered dial tone for phones without a visual indicator
Call waiting	When a user is on a call, and a new call comes in, he or she hears an audible tone and can “click over” to the new caller.
Caller ID on call waiting	When a user is on a call, the name of the second caller is announced or the caller ID is shown.

Feature	Description
Transfer	This feature includes both blind and supervised transfers using the standard established by Bellcore laboratories. The flash hook method is common with analog trunks.
Conference	Conference calls are initiated from an analog phone using flash hook or feature access codes.
Speed dial	A user can set up keys for commonly dialed numbers and dial these numbers directly from an analog phone.
Call forward all	Calls can be forwarded to a number within the dial plan.
Redial	A simple last-number redial can be activated from analog phones.
DID	Supported on E&M and FXS DID ports.



Analog Trunks (Cont.)

Inbound and Outbound Caller ID with FXO and FXS

Caller ID Display
Number 408 555-0100
Name ACME Enterprises

Caller ID Display
Number 555-0112
Name John Smith

Extension 0113

08 555-0199

Service Provider Database
Number 408 555-0100
Name ACME Enterprises

Analog Extension
Station ID Number 555-0112
Station ID Name John Smith

CVOICE v6.0—2-18

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

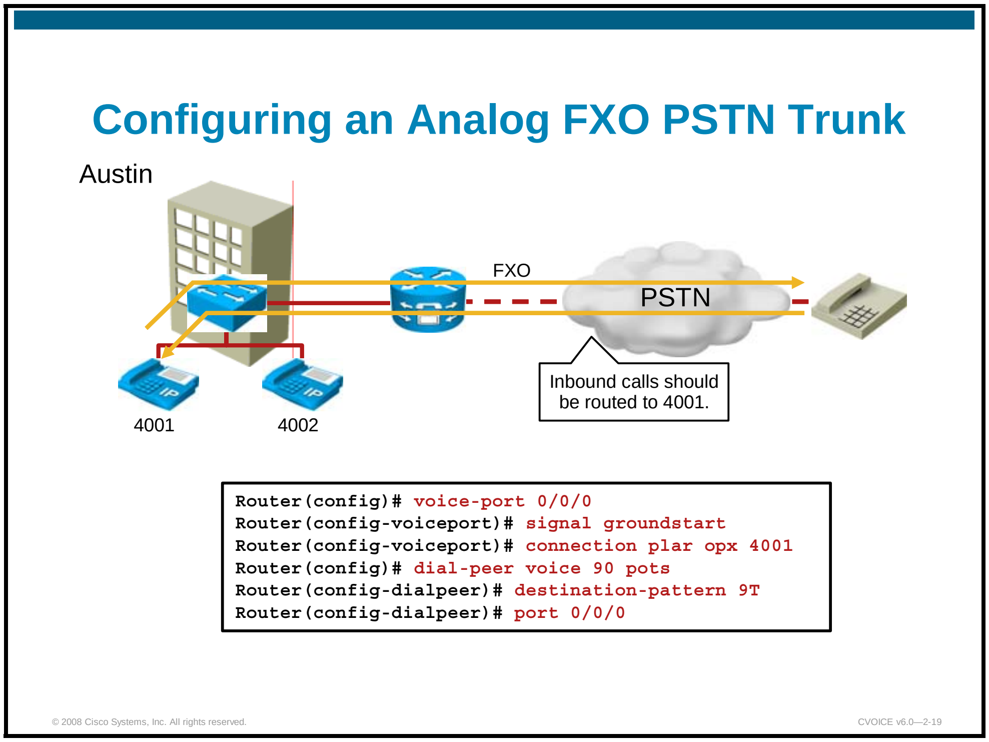
- **Call 1:** Call 1 is from the analog phone to another phone on the premises. The FXS port is configured with a station ID name and station ID number. The name is John Smith, and the number is 555-0112. When a call is placed from the analog phone to another phone on the premises, an IP phone in this case, the caller name and number are displayed on the screen of the IP phone.
- **Call 2:** Call 2 is placed from the same analog phone, but the destination is off the premises of the PSTN. The FXO port forwards the station ID name and station ID number to the CO switch. The CO switch discards the station ID name and station ID number and replaces them with information that it has configured for this connection.

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

Note Although the gateway supports the caller ID feature, Cisco Unified Communications Manager does not support this feature on FXO ports if the gateway is configured for Media Gateway Control Protocol (MGCP).

FXO Port Configuration

This subtopic shows an FXO port configuration.



Configuring an Analog FXO PSTN Trunk

Inbound calls should be routed to 4001.

```
Router(config)# voice-port 0/0/0
Router(config-voiceport)# signal groundstart
Router(config-voiceport)# connection plar opx 4001
Router(config)# dial-peer voice 90 pots
Router(config-dialpeer)# destination-pattern 9T
Router(config-dialpeer)# port 0/0/0
```

CVOICE v6.0—2-19

An FXO trunk is one of the simplest analog trunks available. Because Dialed Number Identification Service (DNIS) can only be sent out to the PSTN, no DID is possible. Automatic Number Identification (ANI) is supported for inbound calls. Two signaling types exist, loop-start and ground-start, with ground-start being the preferred method.

The figure above is an example of a typical FXO trunk configuration.

FXO Port Configuration Example

In this example, you have been assigned to configure a voice gateway to route calls to and from the PSTN through an FXO port on the router. In this scenario, you must set up a private line, automatic ringdown (PLAR) connection using an FXO port that is connected to the PSTN.

The requirements are as follows:

- Configure the voice port to use ground-start signaling
- Configure a PLAR connection from a remote location to extension 4001 in Austin
- Configure a standard dial peer for inbound and outbound PSTN calls

Because an FXO trunk does not support DID, two-stage dialing is required for all inbound calls. If all inbound calls should be routed to a specific extension (for example, a front desk), you can use the **connection plar opx** command. In this example, all inbound calls are routed to extension 4001.

Complete these steps to configure an FXO voice port.

Step 1 Enter voice-port configuration mode.

```
Router(config# voice-port 0/0/0
```

Step 2 Select the access signaling type to match that of the telephony connection that you are making.

```
Router(config-voiceport)# signal ground-start
```

Step 3 Specify a PLAR Off-Premises eXtension (OPX) connection.

```
Router(config-voiceport)# connection plar opx 4001
```

PLAR is an autodialing mechanism that permanently associates a voice interface with a far-end voice interface, allowing call completion to a specific telephone number or PBX without dialing. 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.

Using the **opx** option, the local voice port provides a local response before the remote voice port receives an answer. On FXO interfaces, the voice port does not answer until the remote side has answered.

Step 4 Activate the voice port.

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

Step 5 Exit voice-port configuration mode.

```
Router(config-voiceport)# exit
```

Step 6 Create a standard dial peer for inbound and outbound PSTN calls.

```
Router(config)# dial-peer voice 90 pots
```

Step 7 Specify the destination pattern.

```
Router(config-dialpeer)# destination-pattern 9T
```

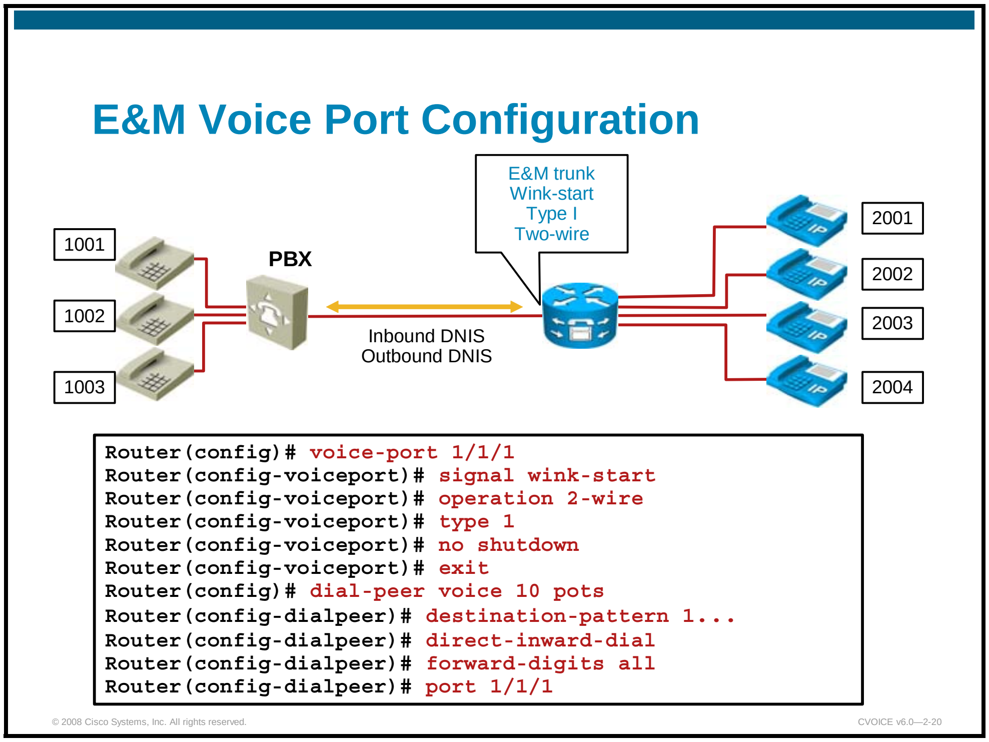
The **T** control character indicates that the **destination-pattern** value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

Step 8 Specify the voice port associated with this dial peer.

```
Router(config-dialpeer)# port 0/0/0
```

E&M Voice Port Configuration

This subtopic covers E&M voice port configuration.



E&M Voice Port Configuration

```
Router(config)# voice-port 1/1/1
Router(config-voiceport)# signal wink-start
Router(config-voiceport)# operation 2-wire
Router(config-voiceport)# type 1
Router(config-voiceport)# no shutdown
Router(config-voiceport)# exit
Router(config)# dial-peer voice 10 pots
Router(config-dialpeer)# destination-pattern 1...
Router(config-dialpeer)# direct-inward-dial
Router(config-dialpeer)# forward-digits all
Router(config-dialpeer)# port 1/1/1
```

CVOICE v6.0—2-20

Configuring an E&M analog trunk is straightforward. Three key options have to be set:

- The signaling E&M signaling type
- Two- or four-wire operation
- The E&M type

The figure shows an example of an E&M port that provides connectivity to a PBX.

E&M Configuration Example

In this example, you have been assigned to configure a voice gateway to work with an existing PBX system according to network requirements. In this scenario, you must set up a voice gateway to interface with a PBX to allow the IP phones to call the POTS phones using a four digit extension.

The requirements are as follows:

- Configure the voice port to use wink-start signaling
- Configure the voice port to use two-wire operation mode
- Configure the voice port to use Type I E&M signaling
- Configure a standard dial peer for the POTS phones behind the PBX

Both sides of the trunk need to have a matching configuration. This example configuration shows an E&M trunk using wink-start signaling, E&M Type I, and two-wire operation. Because E&M supports inbound and outbound DNIS, DID is also configured on the corresponding dial peer.

Complete these steps to configure an E&M voice port.

Step 1 Enter voice-port configuration mode.

Step 2 Select the access signaling type to match that of the telephony connection that you are making.

```
Router(config-voiceport)# signal wink-start
```

Step 3 Select a specific cabling scheme for the E&M port.

```
Router(config-voiceport)# operation 2-wire
```

This command affects only voice traffic. If the wrong cable scheme is specified, the user might get voice traffic in only one direction.

Note Using this command on a voice port changes the operation of both voice ports on a voice port module (VPM) card. The voice port must be shut down and then opened again for the new value to take effect.

Step 4 Specify the type of E&M interface.

```
Router(config-voiceport)# type 1
```

Step 5 Activate the voice port.

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

Step 6 Exit voice-port configuration mode.

```
Router(config-voiceport)# exit
```

Step 7 Create a dial peer for the POTS phones.

```
Router(config)# dial-peer voice 10 pots
```

Step 8 Specify the destination pattern for the POTS phones.

```
Router(config-dialpeer)# destination-pattern 1...
```

Step 9 Specify DID.

```
Router(config-dialpeer)# direct-inward-dial
```

Note DID is needed when POTS phones call IP phones. In this case, match the POTS dial peer. This same dial peer is also used to call out to POTS phones

Step 10 Specify digit forwarding all.

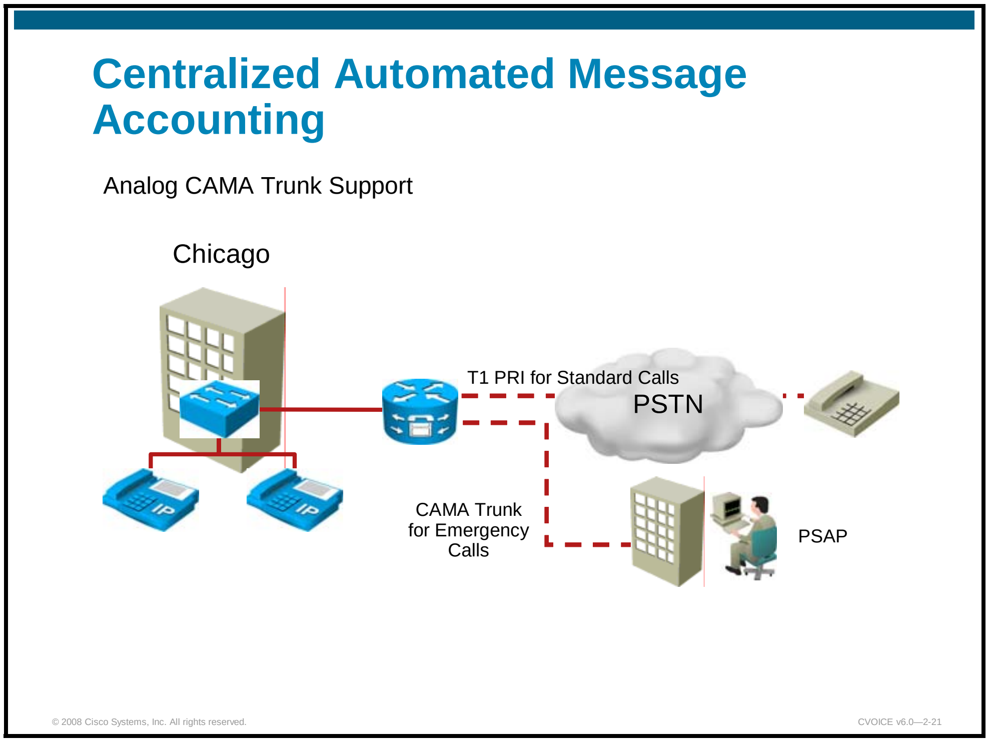
```
Router(config-dialpeer)# forward-digits all
```

Step 11 Specify the voice port that is associated with this dial peer.

```
Router(config-dialpeer)# port 1/1/1
```

Centralized Automated Message Accounting

This topic describes Centralized Automated Message Accounting (CAMA).



Centralized Automated Message Accounting

Analog CAMA Trunk Support

CVOICE v6.0—2-21

A CAMA trunk is a special analog trunk type that was originally developed for long-distance billing but is now mainly used for emergency call services (911 and E911 services). Use CAMA ports to connect to a public safety answering point (PSAP) for emergency calls. A CAMA trunk can only send outbound ANI information, which is required by the local PSAP.

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

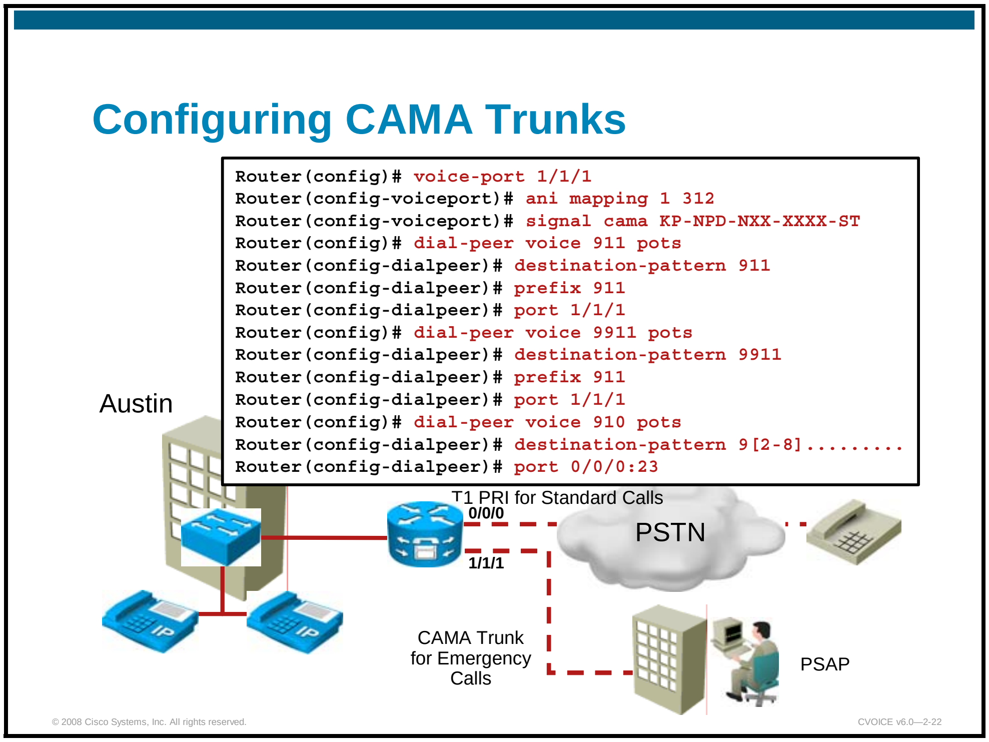
- The calling number is used to reference the Automatic Location Identification (ALI) database to find the exact location of the caller and any extra information about the caller that may have been stored in the database.
- The calling number is used as a callback number in case the call is disconnected.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

Note	You must check local legal requirements when using CAMA.

The diagram above shows a voice gateway connecting an enterprise to an E911 network. Calls to emergency services are routed based on the calling number, not the called number. The calling number is checked against a database of emergency service providers that cross-references the service providers for the caller location. When this information is determined, the call is then routed to the proper PSAP, which dispatches services to the caller location.

During the setup of an E911 call, before the audio channel is connected, the calling number is transmitted to each switching point, known as a selective router, via CAMA.

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



Configuring CAMA Trunks

```
Router(config)# voice-port 1/1/1
Router(config-voiceport)# ani mapping 1 312
Router(config-voiceport)# signal cama KP-NPD-NXX-XXXX-ST
Router(config)# dial-peer voice 911 pots
Router(config-dialpeer)# destination-pattern 911
Router(config-dialpeer)# prefix 911
Router(config-dialpeer)# port 1/1/1
Router(config)# dial-peer voice 9911 pots
Router(config-dialpeer)# destination-pattern 9911
Router(config-dialpeer)# prefix 911
Router(config-dialpeer)# port 1/1/1
Router(config)# dial-peer voice 910 pots
Router(config-dialpeer)# destination-pattern 9[2-8].........
Router(config-dialpeer)# port 0/0/0:23
```

CVOICE v6.0—2-22

This diagram shows a site that has a T1 PRI circuit for normal inbound and outbound PSTN calls. Because the local PSAP requires a dedicated CAMA trunk for emergency (911) calls, all emergency calls are routed using a dial peer pointing to the CAMA trunk.

The voice port 1/1/1 is the CAMA trunk. The actual configuration depends on the PSAP requirements. In this case, the digit 1 is used to signal the area code 312. The voice port is then configured for CAMA signaling using the **signal cama** command. Four options exist:

- **KP-0-NXX-XXXX-ST:** 7-digit ANI transmission. The Numbering Plan Area (NPA) or area code is implied by the trunk group and is not transmitted.
- **KP-0-NPA-NXX-XXXX-ST:** 10-digit transmission. The E.164 number is fully transmitted.
- **KP-0-NPA-NXX-XXXX-ST-KP-YYY-YYY-YYYY-ST:** Supports CAMA signaling with ANI and Pseudo ANI (PANI).
- **KP-2-ST:** Default transmission when the CAMA trunk cannot get a corresponding Numbering Plan Digit (NPD) in the lookup table, or when the calling number is fewer than 10 digits. (NPA digits are not available.)
- **KP-NPD-NXX-XXXX-ST:** 8-digit ANI transmission, where the NPD is a single MF digit that is expanded into the NPA. The NPD table is preprogrammed in the sending and receiving equipment (on each end of the MF trunk); for example: 0 = 415, 1 = 510, 2 = 650, and 3 = 916, so 05551234 = 415 555-1234, 15551234 = 510 555-1234, and so on. The NPD value range is 0 to 3.

When you use the NPD format, the area code needs to be associated with a single digit. You can preprogram the NPA, or area code, into a single MF digit using the **ani mapping** voice port command. The number of programmed NPDs is determined by local policy as well as by the number of NPAs that the PSAP serves. Repeat this command until all NPDs are configured or until the NPD maximum range is reached.

In this example, the PSAP expects NPD signaling, with the area code 312 being represented by the digit 1.

Complete these steps to configure a CAMA trunk.

Step 1 Configure a voice port for 911 calls.

```
Router(config)# voice-port 1/1/1
Router(config-voiceport)# ani mapping 1 312
Router(config-voiceport)# signal cama kp-npd-nxx-xxxx-st
```

Step 2 Configure a dedicated dial peer to route emergency calls using the CAMA trunk when a user dials “911”.

```
Router(config)# dial-peer voice 911 pots
Router(config-dialpeer)# destination-pattern 911
Router(config-dialpeer)# prefix 911
Router(config-dialpeer)# port 1/1/1
```

Step 3 Configure a dedicated “9911” dial peer to route all emergency calls using the CAMA trunk when a user dials “9911”.

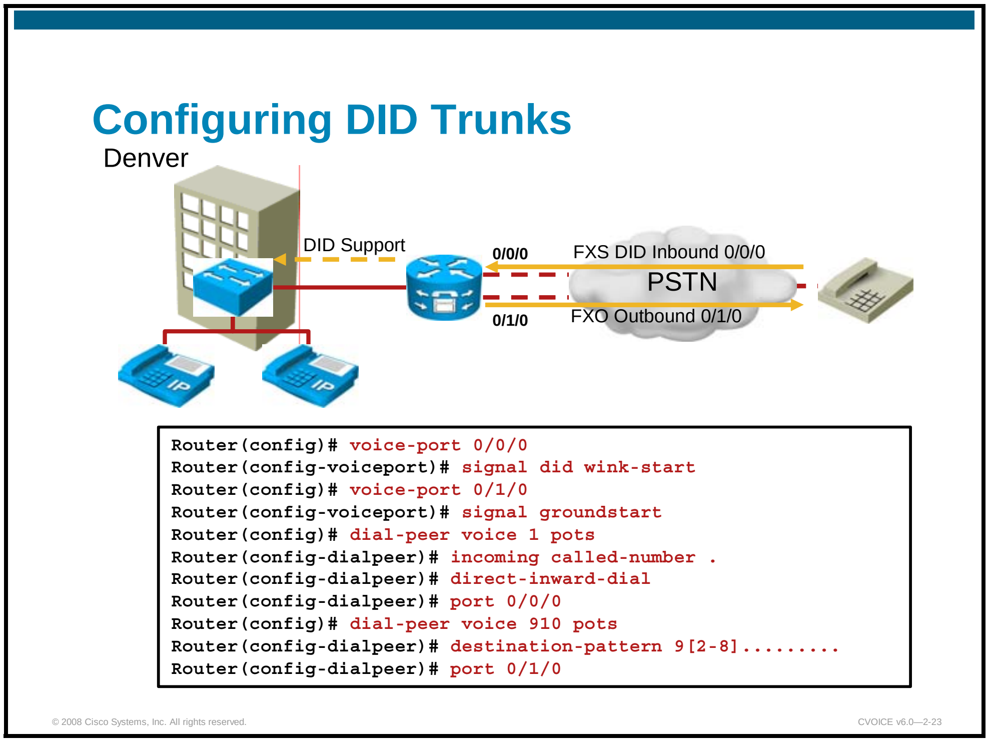
```
Router(config)# dial-peer voice 9911 pots
Router(config-dialpeer)# destination-pattern 9911
Router(config-dialpeer)# prefix 911
Router(config-dialpeer)# port 1/1/1
```

Step 4 Configure a standard PSTN dial peer for all other inbound and outbound PSTN calls.

```
Router(config)# dial-peer voice 910 pots
Router(config-dialpeer)# destination-pattern 9[2-8].........
Router(config-dialpeer)# port 0/0/0:23
```

Direct Inward Dialing

This topic describes how to configure a voice port for DID.



Configuring DID Trunks

```
Router(config)# voice-port 0/0/0
Router(config-voiceport)# signal did wink-start
Router(config)# voice-port 0/1/0
Router(config-voiceport)# signal groundstart
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer)# incoming called-number .
Router(config-dialpeer)# direct-inward-dial
Router(config-dialpeer)# port 0/0/0
Router(config)# dial-peer voice 910 pots
Router(config-dialpeer)# destination-pattern 9[2-8].........
Router(config-dialpeer)# port 0/1/0
```

Typically, FXS ports connect to analog phones, but some carriers offer FXS trunks, which support DID. The DID service is offered by telephone companies, and it enables callers to dial an extension directly on a PBX or a VoIP system (for example, Cisco Unified Communications Manager and Cisco IOS routers and gateways) without the assistance of an operator or automated call attendant. This service makes use of DID trunks, which forward only the last three to five digits of a phone number to the PBX, router, or gateway. For example, a company has phone extensions 555-0100 to 555-0199. A caller dials 555-0123 and the local CO forwards 123 to the PBX or VoIP system. The PBX or VoIP system then rings extension 123. This entire process is transparent to the caller.

An FXS DID trunk can only receive inbound calls, thus a combination of FXS DID and FXO ports is required for inbound and outbound calls. Two signaling types exist, loop-start and ground-start, with ground-start being the preferred method.

The diagram in the figure shows an analog trunk using an FXS DID trunk for inbound calls and a standard FXO trunk for outbound calls.

Follow these steps to enable DID signaling on a FXS port.

Step 1 Configure the FXS port for DID and wink-start.

```
Router(config)# voice-port 0/0/0
Router(config-voiceport)# signal did wink-start
```

Step 2 Configure the FXO port for ground-start signaling.

```
Router(config)# voice-port 0/1/0
Router(config-voiceport)# signal groundstart
```

Step 3 Create an inbound dial peer using the FXS DID port. Note that direct inward dialing is enabled.

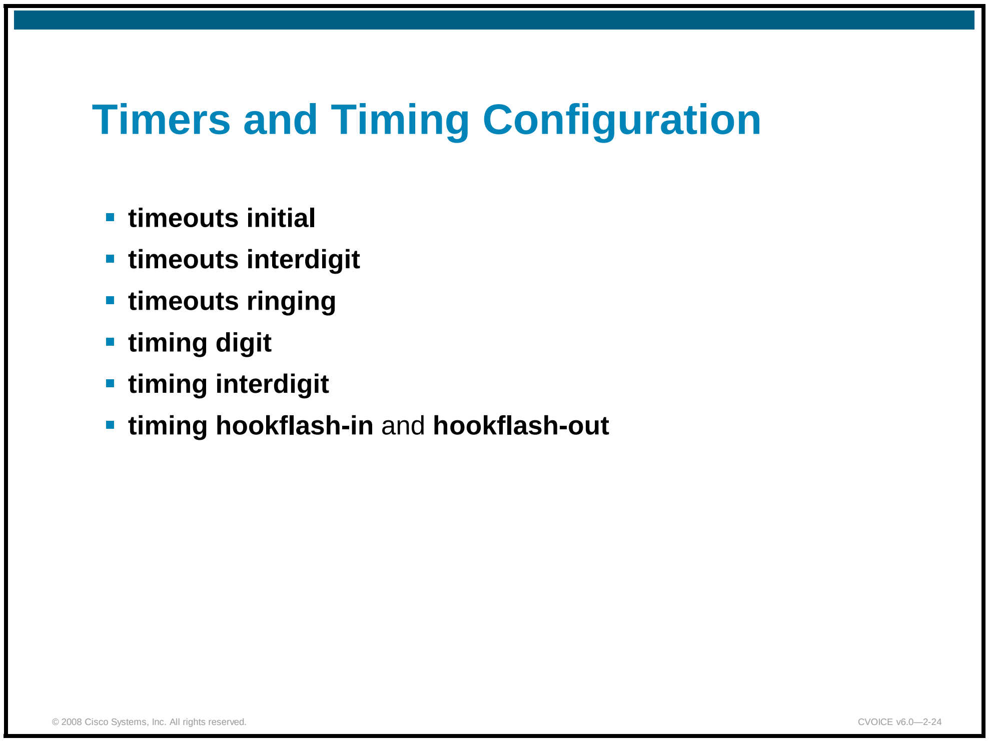
```
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer)# incoming called-number .
Router(config-dialpeer)# direct-inward-dial
Router(config-dialpeer)# port 0/0/0
```

Step 4 Create a standard outbound dial peer using the FXO port.

```
Router(config)# dial-peer voice 910 pots
Router(config-dialpeer)# destination-pattern 9[2-8].........
Router(config-dialpeer)# port 0/1/0
```

Timers and Timing Configuration

This topic describes timing configuration parameters on voice ports.



Timers and Timing Configuration

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

CVOICE v6.0—2-24

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

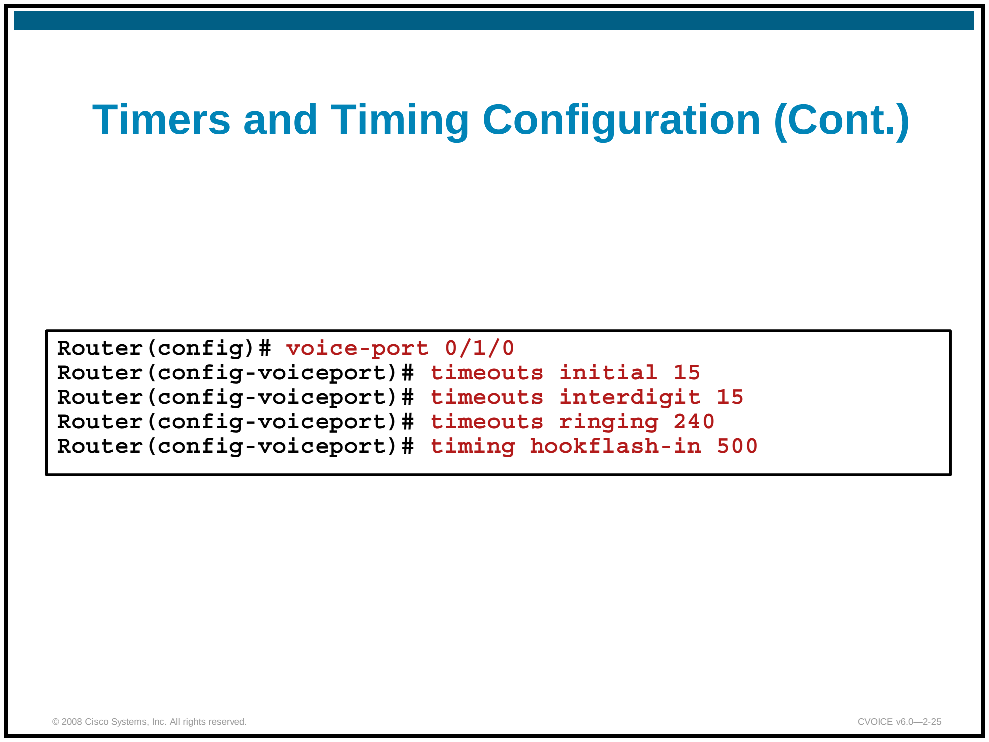
- **timeouts initial:** Configures the initial digit timeout value in seconds. This value controls how long the dial tone is presented before the first digit is expected. This timer value typically does not need to be changed.
- **timeouts interdigit:** Configures the number of seconds the system will wait between caller-entered digits before sending the input to be assessed. If the digits are coming from an automated device, and the dial plan is variable-length, you can shorten this timer so that the call proceeds without waiting the full default of 10 seconds for the interdigit timer to expire.
- **timeouts ringing:** Configures the length of time that a caller may continue to let the telephone ring when there is no answer. You can configure this setting to be less than the default of 180 seconds so that you do not tie up the voice port when it is evident that the call is not going to be answered.
- **timing digit:** Configures the DTMF digit signal duration for a specified voice port. You can use this setting to fine-tune a connection to a device that may have trouble recognizing dialed digits. If a user or device dials too quickly, the digit may not be recognized. By changing the timing on the digit timer, you can provide for a shorter or longer DTMF duration.
- **timing interdigit:** Configures the DTMF interdigit duration for a specified voice port. You can change this setting to accommodate faster or slower dialing characteristics.

- **timing hookflash-in** and **hookflash-out:** Configures the maximum duration (in milliseconds) of a hookflash indication. Hookflash is an indication by a caller that the caller wishes to do something specific with the call, such as transfer the call or place the call on hold. For the **hookflash-in** command, if the hookflash lasts longer than the specified limit, the FXS interface processes the indication as on hook. If you set the value too low, the hookflash may be interpreted as a hang-up; if you set the value too high, the handset has to be left hung up for a longer period to clear the call. For the **hookflash-out** command, the setting specifies the duration (in milliseconds) of the hookflash indication that the gateway generates outbound. You can configure this to match the requirements of the connected device.

  Under normal use, these timers do not need to be adjusted. There are two instances in which these timers can be configured to allow more or less time for a specific function:

  — When ports are connected to a device that does not properly respond to dialed digits or hookflash

  — When the connected device provides automated dialing



Timers and Timing Configuration (Cont.)

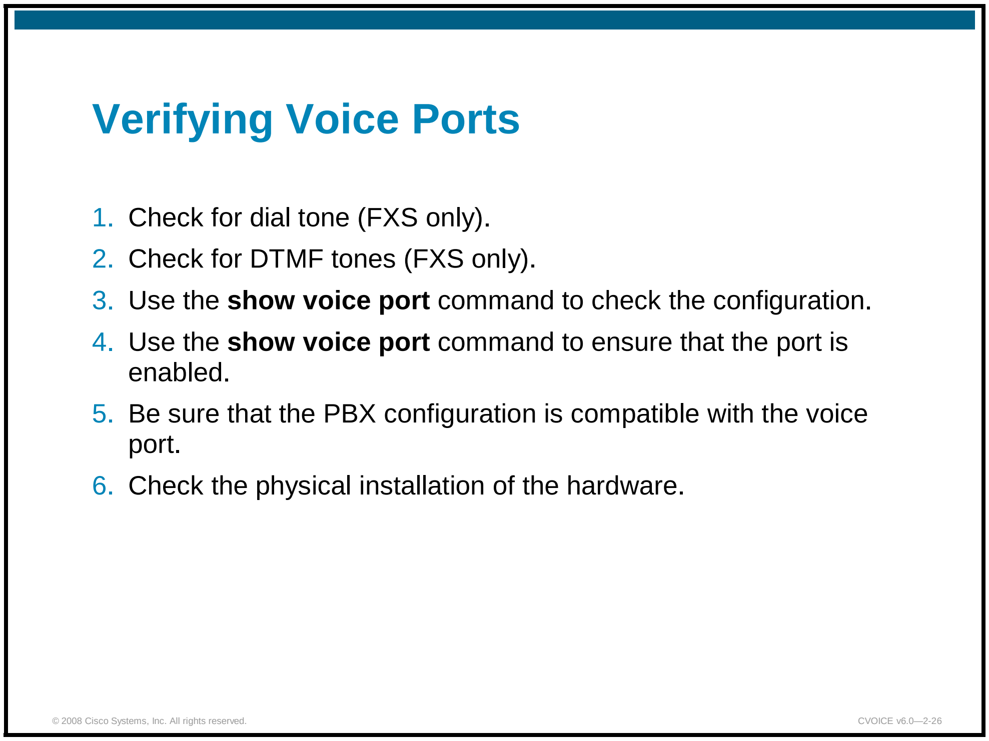
```
Router(config)# voice-port 0/1/0
Router(config-voiceport)# timeouts initial 15
Router(config-voiceport)# timeouts interdigit 15
Router(config-voiceport)# timeouts ringing 240
Router(config-voiceport)# timing hookflash-in 500
```

CVOICE v6.0—2-25

The installation that is shown in the figure is for a home for someone who may require more time to dial digits. The requirement to allow the telephone to ring, unanswered, for 4 minutes allows more time for the telephone to be answered. The configuration in the figure enables several timing parameters on a Cisco voice-enabled router voice port 0/1/0. The initial timeout is lengthened to 15 seconds, the interdigit timeout is lengthened to 15 seconds, the ringing timeout is set to 240 seconds, and the hookflash-in parameter is set to 500 ms.

Verifying Voice Ports

This topic describes how to use **show**, **test**, and **debug** commands to monitor and troubleshoot voice ports.



Verifying Voice Ports

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

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-26

You can perform these steps to verify voice port configuration:

Step 1 Pick up the handset of an attached telephony device and check for a dial tone. If there is no dial tone, proceed to Step 3.

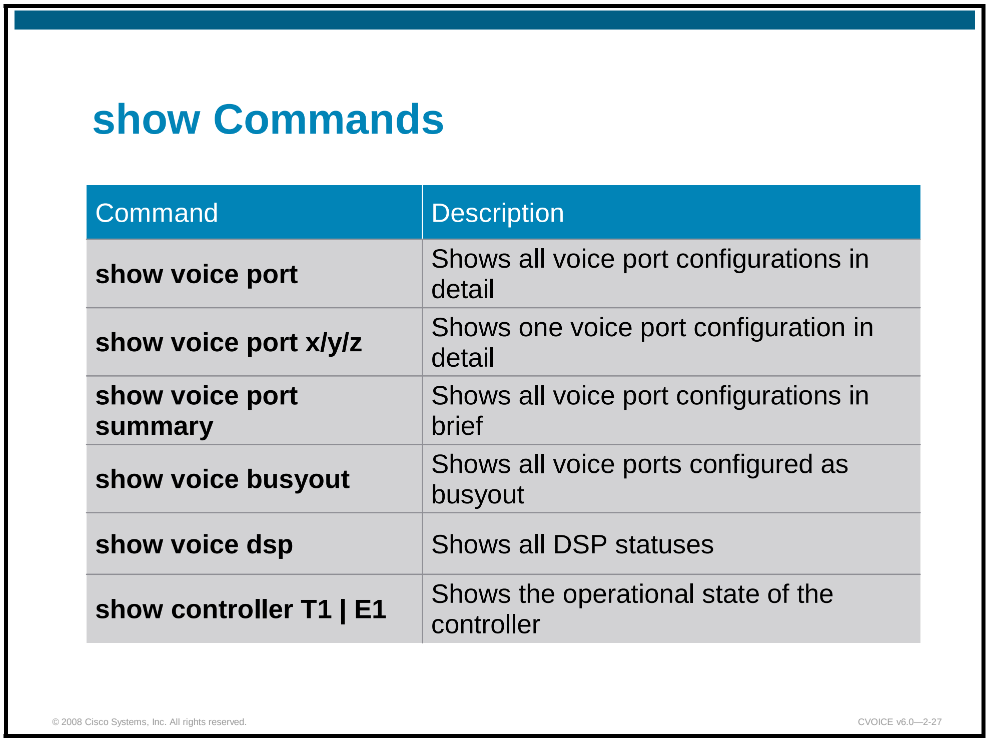
Step 2 If you have a dial tone, check for DTMF voice band tones, such as touch-tone detection. If the dial tone stops when you dial a digit, the voice port is probably configured properly.

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

Step 4 Use the **show voice port** command to make sure that the port is enabled. If the port is administratively down, use the **no shutdown** command. If the port was working previously and is not working now, it is possible that the port is in a hung state. Use the **shutdown** and **no shutdown** commands to reinitialize the port.

Step 5 If you have configured E&M interfaces, make sure that the values associated with your specific PBX are correct. Check for two-wire or four-wire wink-start, immediate-start, or delay-start signaling types, and check the E&M interface type. These parameters need to match those set on the PBX for the interface to communicate properly.

Step 6 You must confirm that the voice network module (VNM) is correctly installed. With the device powered down, remove the VNM and reinsert it to verify the installation. If the device has other slots available, try inserting the VNM into another slot to isolate the problem. Similarly, you must move the voice interface card (VIC) to another VIC slot to determine if the problem is with the VIC or with the module slot.

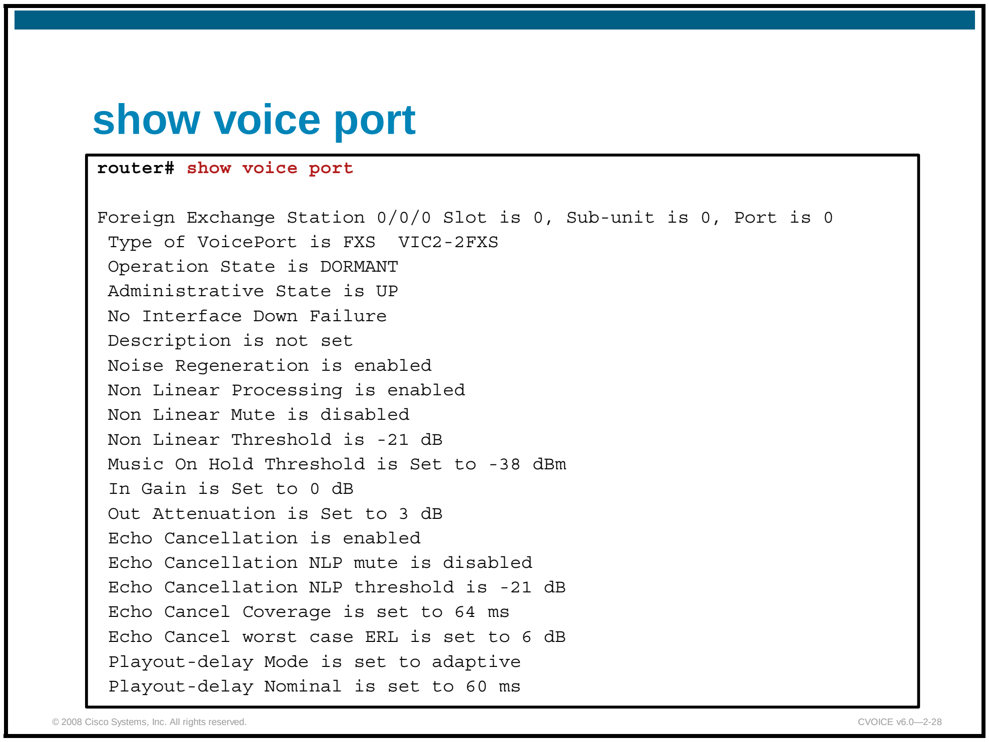


show Commands

Command	Description
show voice port	Shows all voice port configurations in detail
show voice port x/y/z	Shows one voice port configuration in detail
show voice port summary	Shows all voice port configurations in brief
show voice busyout	Shows all voice ports configured as busyout
show voice dsp	Shows all DSP statuses
show controller T1 | E1	Shows the operational state of the controller

CVOICE v6.0—2-27

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

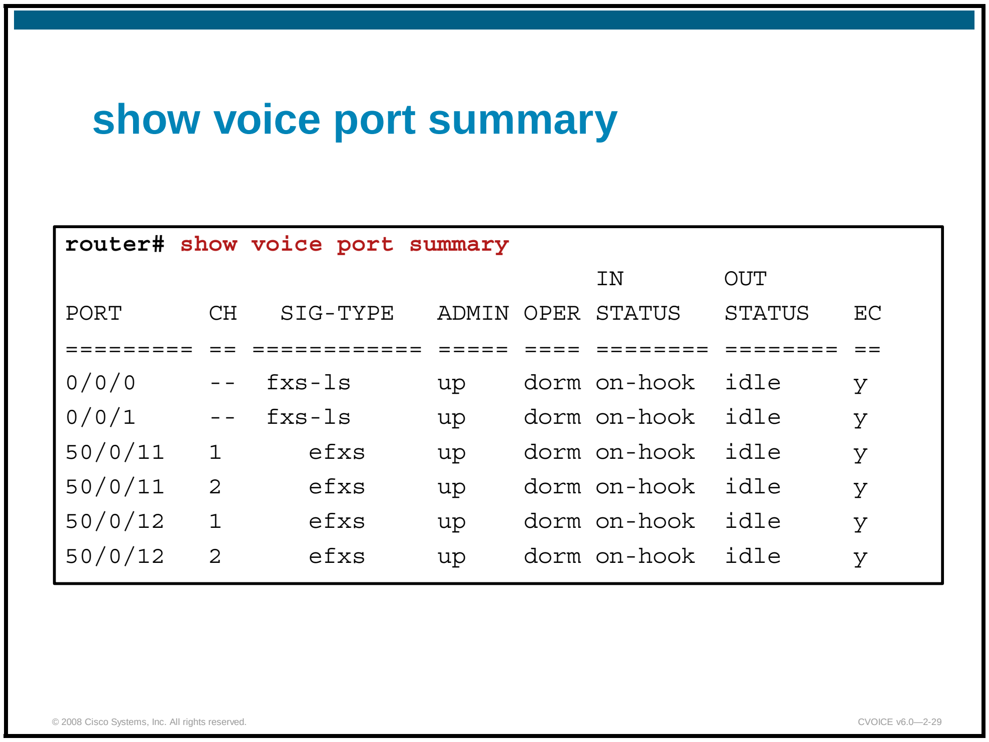


show voice port

```
router# show voice port

Foreign Exchange Station 0/0/0 Slot is 0, Sub-unit is 0, Port is 0
 Type of VoicePort is FXS  VIC2-2FXS
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 3 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 64 ms
 Echo Cancel worst case ERL is set to 6 dB
 Playout-delay Mode is set to adaptive
 Playout-delay Nominal is set to 60 ms
```

CVOICE v6.0—2-28

This figure shows an example of the **show voice port** command.

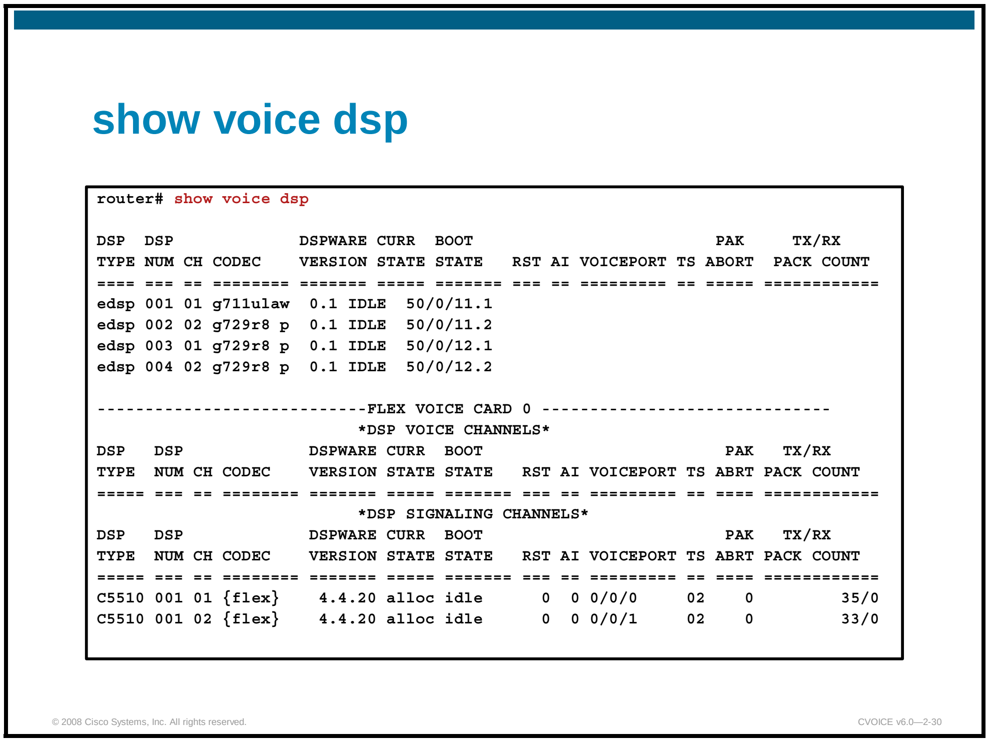


show voice port summary

```
router# show voice port summary
                                     IN       OUT
PORT      CH   SIG-TYPE    ADMIN OPER STATUS   STATUS   EC
========= == ============ ===== ==== ======== ======== ==
0/0/0     --  fxs-ls       up    dorm on-hook  idle     y
0/0/1     --  fxs-ls       up    dorm on-hook  idle     y
50/0/11   1      efxs      up    dorm on-hook  idle     y
50/0/11   2      efxs      up    dorm on-hook  idle     y
50/0/12   1      efxs      up    dorm on-hook  idle     y
50/0/12   2      efxs      up    dorm on-hook  idle     y
```

CVOICE v6.0—2-29

This figure shows an example of the **show voice port summary** command.

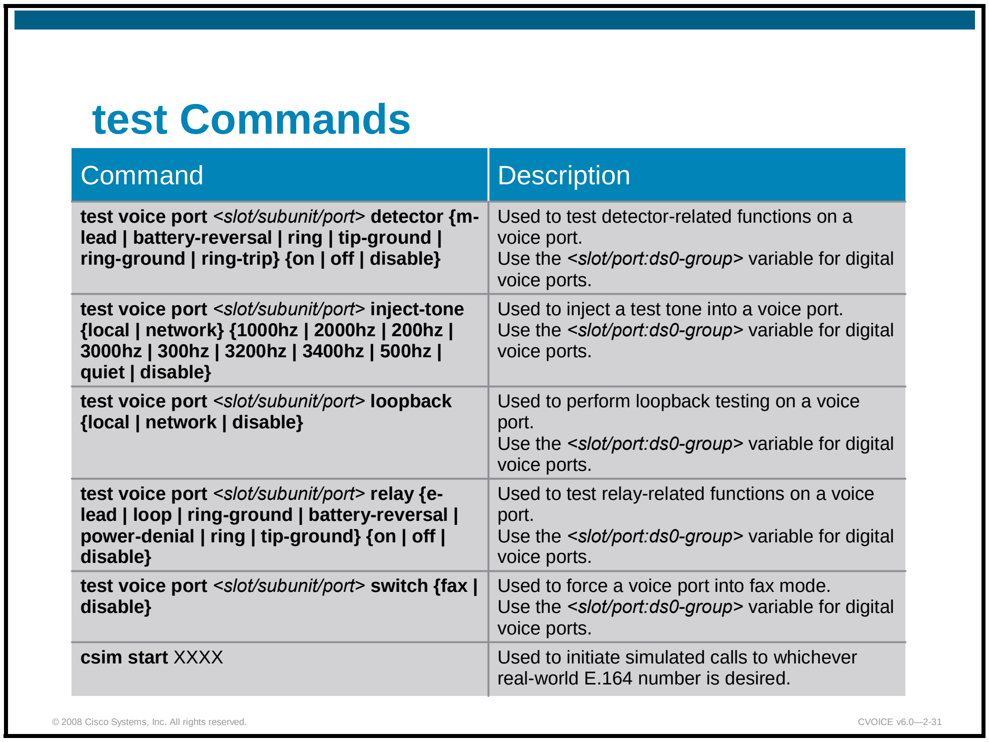


show voice dsp

```
router# show voice dsp

DSP  DSP             DSPWARE CURR  BOOT                         PAK     TX/RX
TYPE NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABORT  PACK COUNT
==== === == ======== ======= ===== ======= === == ========= == ===== ============
edsp 001 01 g711ulaw  0.1 IDLE  50/0/11.1
edsp 002 02 g729r8 p  0.1 IDLE  50/0/11.2
edsp 003 01 g729r8 p  0.1 IDLE  50/0/12.1
edsp 004 02 g729r8 p  0.1 IDLE  50/0/12.2

----------------------------FLEX VOICE CARD 0 ------------------------------
                           *DSP VOICE CHANNELS*
DSP   DSP               DSPWARE CURR  BOOT                         PAK   TX/RX
TYPE  NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ======== ======= ===== ======= === == ========= == ==== ============
                           *DSP SIGNALING CHANNELS*
DSP   DSP               DSPWARE CURR  BOOT                         PAK   TX/RX
TYPE  NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ======== ======= ===== ======= === == ========= == ==== ============
C5510 001 01 {flex}    4.4.20 alloc idle       0  0 0/0/0      02    0          35/0
C5510 001 02 {flex}    4.4.20 alloc idle       0  0 0/0/1      02    0          33/0
```

CVOICE v6.0—2-30

This figure shows an example of the **show voice dsp** command.



test Commands

Command	Description
test voice port <*slot/subunit/port*> **detector {m-lead | battery-reversal | ring | tip-ground | ring-ground | ring-trip} {on | off | disable}**	Used to test detector-related functions on a voice port. Use the <*slot/port:ds0-group*> variable for digital voice ports.
test voice port <*slot/subunit/port*> **inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet | disable}**	Used to inject a test tone into a voice port. Use the <*slot/port:ds0-group*> variable for digital voice ports.
test voice port <*slot/subunit/port*> **loopback {local | network | disable}**	Used to perform loopback testing on a voice port. Use the <*slot/port:ds0-group*> variable for digital voice ports.
test voice port <*slot/subunit/port*> **relay {e-lead | loop | ring-ground | battery-reversal | power-denial | ring | tip-ground} {on | off | disable}**	Used to test relay-related functions on a voice port. Use the <*slot/port:ds0-group*> variable for digital voice ports.
test voice port <*slot/subunit/port*> **switch {fax | disable}**	Used to force a voice port into fax mode. Use the <*slot/port:ds0-group*> variable for digital voice ports.
csim start XXXX	Used to initiate simulated calls to whichever real-world E.164 number is desired.

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

Note The **csim** command is an undocumented command.

The **test** commands provide the ability to analyze and troubleshoot voice ports on the Cisco 2800 Series routers and 3800 Series routers. There are five **test** commands to force voice ports into specific states to test the voice port configuration.

test voice port detector

Use the **test voice port detector** privileged EXEC command to force a detector into specific states for testing. For each signaling type (E&M, FXO, FXS), only the applicable keywords are displayed. When you are finished testing, be sure to enter the command with the **disable** keyword to end the forced state. The **disable** keyword is available only if a test condition is already activated.

test voice port inject-tone

Use the **test voice port inject-tone** privileged EXEC command to inject a test tone or to end a test tone. A call must be established on the voice port under test. When you are finished testing, be sure to enter the **disable** keyword to end the test tone. The **disable** keyword is available only if a test condition is already activated. When you enter the **disable** keyword, you must enter a direction (either **network** or **local**); however, you can enter either direction, regardless of which direction you entered to inject the test tone.

test voice port loopback

Use the **test voice port loopback** privileged EXEC command to initiate or end a loopback at a voice port. A call must be established on the voice port under test. When you are finished testing, be sure to enter the **disable** keyword to end the forced loopback. The **disable** keyword is available only if a test condition is already activated.

test voice port relay

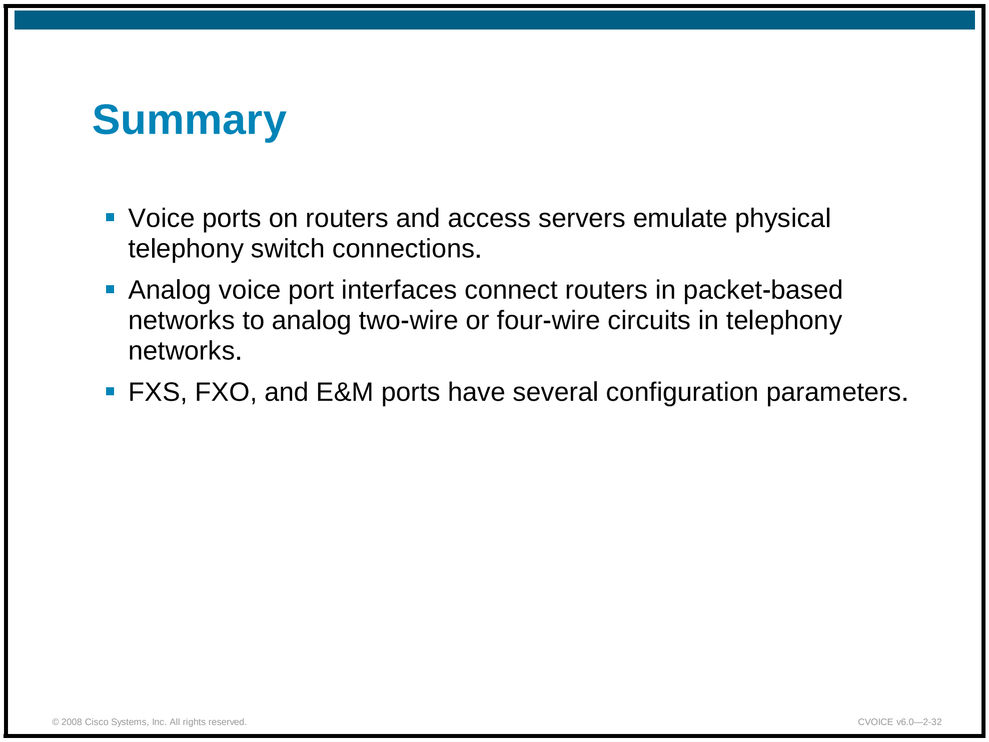
Use the **test voice port relay** privileged EXEC command to force a relay into specific states for testing. For each signaling type (E&M, FXO, FXS), only the applicable keywords are displayed. When you are finished testing, be sure to enter the **disable** keyword to end the forced state. The **disable** keyword is available only if a test condition is already activated.

test voice port switch

Use the **test voice port switch** privileged EXEC command to force a voice port into fax mode for testing. If no fax data is detected by the voice port, the voice port remains in fax mode for 30 seconds and then reverts automatically to voice mode. After you enter the **test voice port switch fax** command, you can use the **show voice call** or **show voice call summary** command to check whether the voice port is able to operate in fax mode. The **disable** keyword ends the forced mode switch; however, the fax mode ends automatically after 30 seconds. The **disable** keyword is available only while the voice port is in fax mode.

Summary

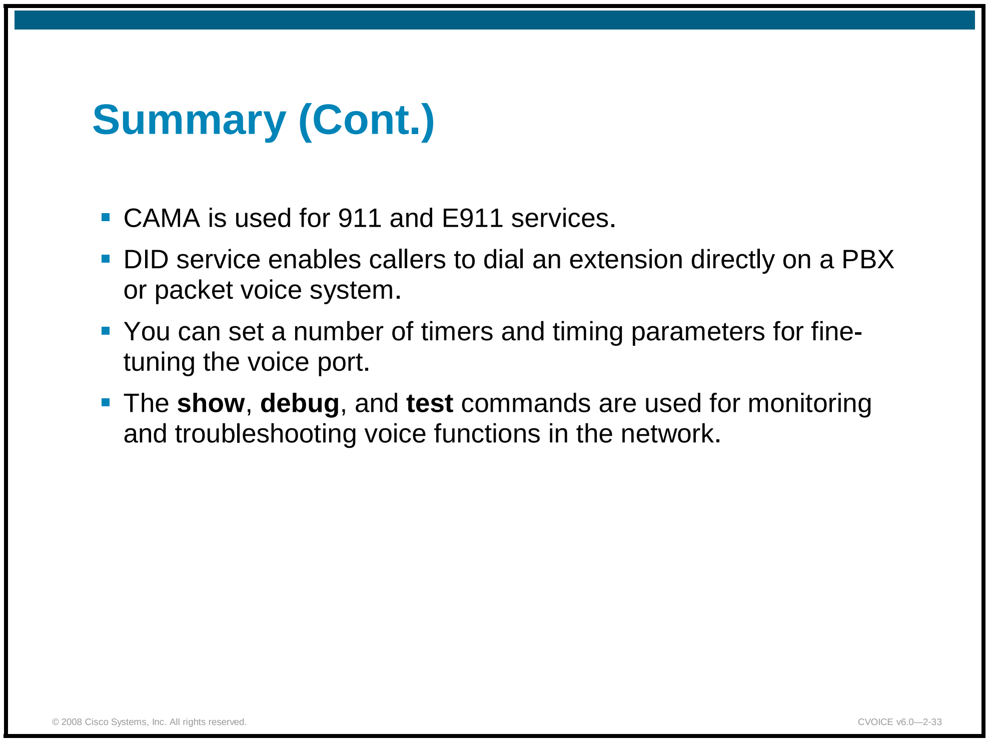
This topic summarizes the key points that were discussed in this lesson.



Summary

- Voice ports on routers and access servers emulate physical telephony switch connections.
- Analog voice port interfaces connect routers in packet-based networks to analog two-wire or four-wire circuits in telephony networks.
- FXS, FXO, and E&M ports have several configuration parameters.

CVOICE v6.0—2-32



Summary (Cont.)

- CAMA is used for 911 and E911 services.
- DID service enables callers to dial an extension directly on a PBX or packet voice system.
- You can set a number of timers and timing parameters for fine-tuning the voice port.
- The **show**, **debug**, and **test** commands are used for monitoring and troubleshooting voice functions in the network.

CVOICE v6.0—2-33

Lesson Self-Check

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

Q1) Voice ports on routers and access servers emulate physical ____________ switch connections.

Relates to: Voice Ports

Q2) What is the best description of supervisory disconnect signaling?

Relates to: Analog Voice Ports

A) a power denial from the switch that lasts at least 350 ms
B) a disconnect message manually sent by the network administrator
C) signaling used by the main voice port of the PBX switch
D) a disconnect process overseen by the network administrator

Q3) Which type of signaling is used when a router provides a current on the E-lead as soon as it sees a current on the M-lead?

Relates to: Analog Voice Ports

A) delay-start signaling
B) immediate-start signaling
C) wink-start signaling
D) QSIG

Q4) Which configuration parameter sets the dial tone, busy tone, and ring back tone?

Relates to: Configuring Analog Voice Ports

A) **cptone**
B) **ring frequency**
C) **ring cadence**
D) **description**
E) **signal**

Q5) A CAMA trunk is a special analog trunk type that was originally developed for long-distance billing but is now mainly used for___________________________.

Relates to: Centralized Automated Message Accounting

Q6) The __________service is offered by telephone companies, and it enables callers to dial an extension directly on a PBX or a VoIP system.

Relates to: Direct Inward Dialing

Q7) Which parameter should be configured when you want to set a limit on the number of seconds to wait between dialed digits before digit input evaluation?

Relates to: Timers and Timing

A) **timeouts initial**
B) **timeouts interdigit**
C) **timing digit**
D) **timing interdigit**

Q8) What is the default setting for the **timeouts ringing** configuration parameter?

Relates to: Timers and Timing

A) 15 seconds
B) 60 seconds
C) 100 seconds
D) 180 seconds

Q9) Which command can you use to check whether the voice port can operate in fax mode after you have entered the **test voice port switch fax** command?

Relates to: Verifying Voice Ports

A) **show voice port**
B) **show voice call**
C) **show fax port**
D) **show switch call**
E) **show fax call**

Q10) Which two conditions can be checked by using the **show voice port** command? (Choose two.)

Relates to: Verifying Analog Voice Ports

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 T1 controller is working properly.

Lesson Self-Check Answer Key

Q1)	telephony
Q2)	A
Q3)	B
Q4)	A
Q5)	emergency call services such as 911 and E911
Q6)	DID
Q7)	B
Q8)	D
Q9)	B
Q10)	A, B

Lesson 3

Understanding Dial Peers

Overview

As a call is being set up across the network, the existence of various parameters is checked and negotiated. A mismatch in parameters can cause call failure. It is important to understand how routers interpret call legs and how call legs relate to inbound and outbound dial peers. Successful implementation of a 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. This lesson also describes call flows as they relate to inbound and outbound dial peers, voice dial peers, hunt groups, digit manipulation, and the matching of calls to dial peers.

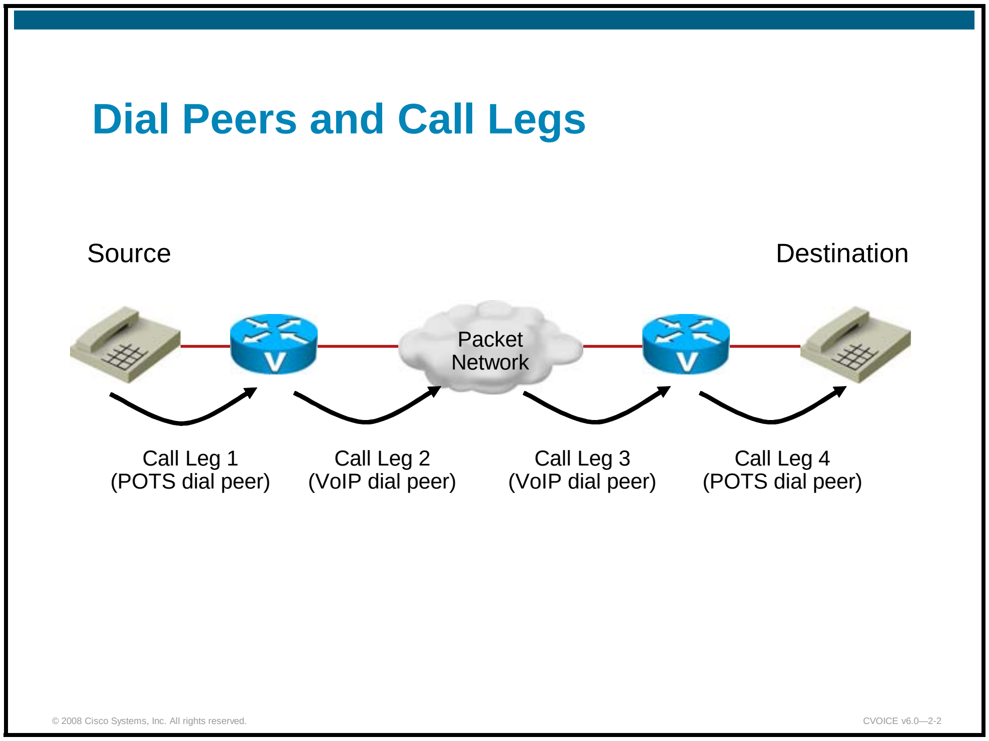
Objectives

Upon completing this lesson, you will be able to describe the purpose and use of dial peers in VoIP. This ability includes being able to meet these objectives:

- Describe POTS and VoIP dial peers and call legs in relation to a simple VoIP network
- Describe how gateways interpret call legs to establish end-to-end calls
- Describe the function of the POTS, VoIP, and default dial peers
- Describe how to configure POTS dial peers
- Describe how to configure VoIP dial peers
- Explain how destination-pattern options associate a telephone number with a given dial peer
- Describe how the router matches inbound dial peers
- Describe the default dial peer
- Describe how the router matches outbound dial peers

Dial Peers and Call Legs

This topic describes the functions of plain old telephone service (POTS) and VoIP dial peers and call legs as components of a simple VoIP network.



Dial Peers and Call Legs

Source

Destination

Packet Network

Call Leg 1 (POTS dial peer)

Call Leg 2 (VoIP dial peer)

Call Leg 3 (VoIP dial peer)

Call Leg 4 (POTS dial peer)

CVOICE v6.0—2-2

Configuring dial peers is the key to implementing dial plans and providing voice services over an IP packet network. Dial peers are used to identify call source and destination endpoints and to define the characteristics that are applied to each call leg in the call connection.

A traditional voice call over the public switched telephone network (PSTN) uses a dedicated 64-kb/s end-to-end circuit. In contrast, a voice call over the packet network is made up of discrete segments or call legs. A call leg is a logical connection between two routers or between a router and a telephony device. A voice call consists of four call legs: two from the perspective of the originating router and two from the perspective of the terminating router, as shown in the diagram in the figure.

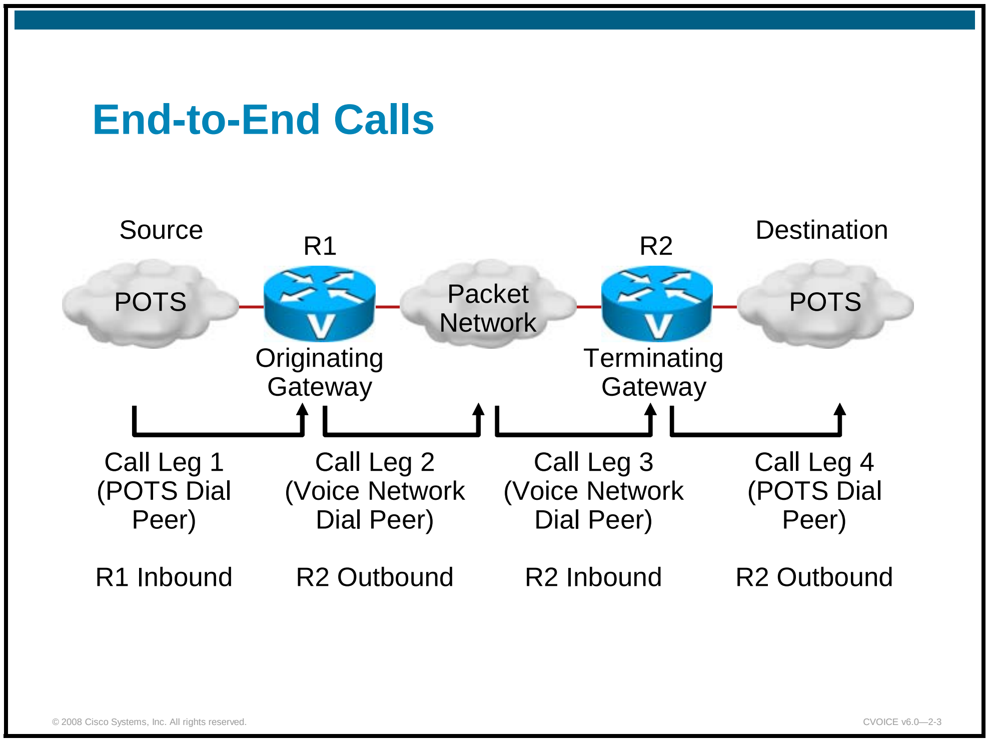
A dial peer is associated with each call leg. Attributes that are defined in a dial peer and applied to that call leg include coder-decoders (codecs), quality of service (QoS), voice activity detection (VAD), and fax rate. A dial peer must be completed for each call leg.

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. The connection is enabled when you have configured dial peers on each interface.

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

End-to-End Calls

This topic describes how gateways interpret call legs to establish end-to-end calls.



End-to-End Calls

Source

R1

R2

Destination

POTS

Packet Network

POTS

Originating Gateway

Terminating Gateway

Call Leg 1 (POTS Dial Peer)

Call Leg 2 (Voice Network Dial Peer)

Call Leg 3 (Voice Network Dial Peer)

Call Leg 4 (POTS Dial Peer)

R1 Inbound

R2 Outbound

R2 Inbound

R2 Outbound

CVOICE v6.0—2-3

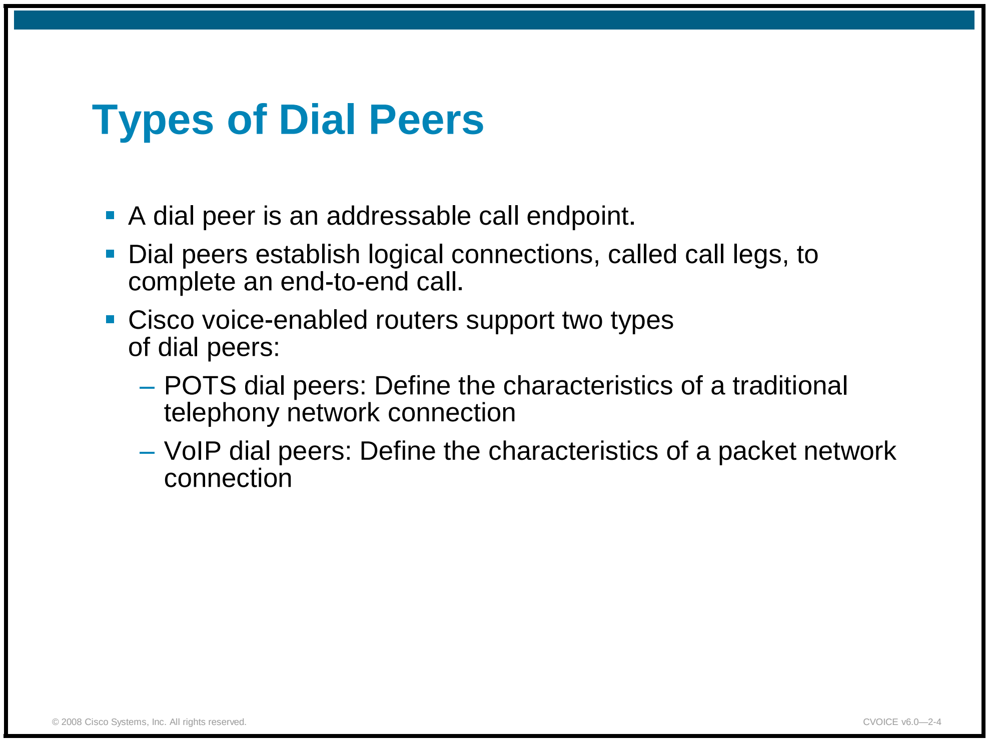
An end-to-end voice call consists of four call legs: two from the originating router (shown as R1 in the figure) or gateway perspective, and two from the terminating router (R2) or gateway perspective. An inbound call leg occurs when an incoming call comes *into* the router or gateway. An outbound call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

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

1. The POTS call arrives at R1 and is associated with a matching inbound POTS dial peer.
2. R1 creates an inbound POTS call leg and assigns it a call ID (call leg 1).
3. R1 associates the dialed string to a matching outbound voice network dial peer.
4. R1 creates an outbound voice network call leg and assigns it a call ID (call leg 2).
5. The voice network call request arrives at R2 and is associated with a matching inbound voice network dial peer.
6. 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.
7. R2 uses the dialed string to match an outbound POTS dial peer.
8. After associating the incoming call setup with an outbound POTS dial peer, R2 creates an outbound POTS call leg, assigns it a Call ID, and completes the call (call leg 4).

Types of Dial Peers

This topic describes functions of the POTS, VoIP, and default dial peers.



Types of Dial Peers

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

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-4

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

A dial peer is an addressable call endpoint. An address, which is called a destination pattern, is configured in every dial peer. Destination patterns can point to just one 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, which are known as call legs, are established in both an inbound and an outbound direction.

Dial peers define the parameters in each call leg for the calls that they match. For example, if a call is originating and terminating at the same site and is not crossing through high-volume WAN links, the call can cross the local network uncompressed and without special priority. A call that originates locally and crosses the WAN link to a remote site may require compression with a specific codec. This call may also require that VAD be turned on. It will definitely need to receive preferential treatment by specifying a higher priority level.

Depending on the call leg, a call is routed using one of the two types of dial peers:

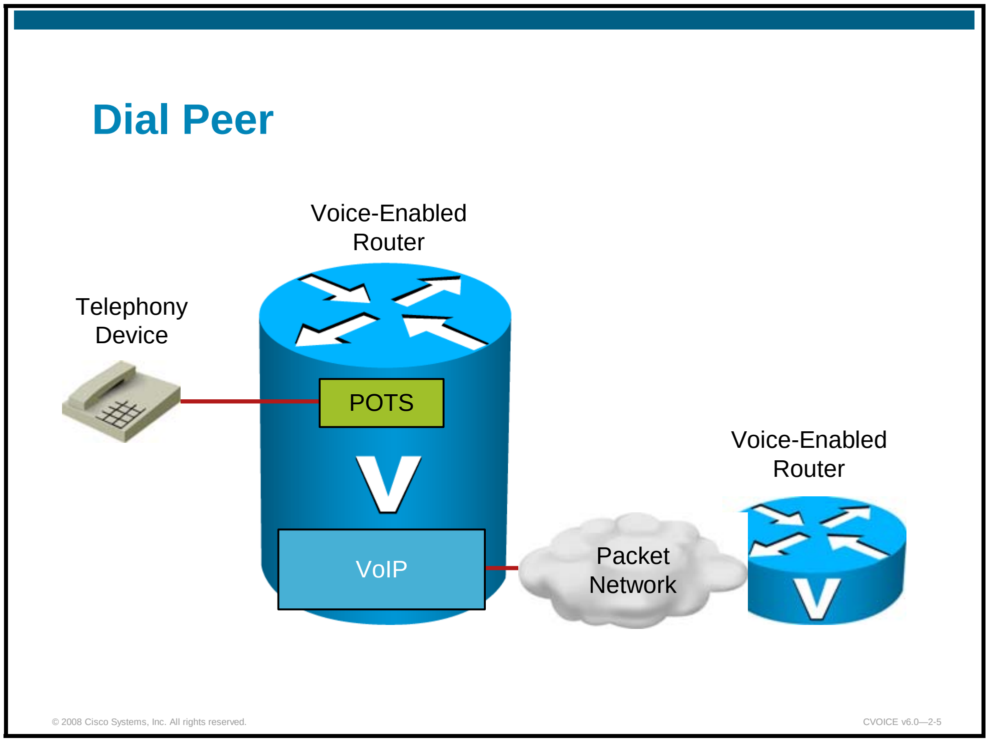
- **POTS dial peers:** Retain the characteristics of a traditional telephony network connection. POTS dial peers map a dialed string to a specific voice port on the local router, normally the voice port connecting the router to the local PSTN, PBX, or telephone.
- **Voice network (or VoIP) dial peers:** Are components on an IP network to which a voice gateway router points via the component IP address that is specified in the **session-target** command for a particular matching dial peer. The four types of voice network dial peers, VoIP, Voice over ATM (VoATM), Voice over Frame Relay (VoFR), and Multimedia Mail over IP (MMoIP), are determined according to the given packet network technology and are described as follows:
  - **VoIP:** Points to the IP address of the destination router that terminates the call.
  - **VoFR:** Points to the data-link connection identifier (DLCI) of the interface from which the call exits the router.
  - **VoATM:** Points to the ATM virtual circuit for the interface from which the call exits the router.
  - **MMoIP:** Points to the e-mail address of the Simple Mail Transfer Protocol (SMTP) server. This type of dial peer is used only for fax traffic.

Tip If you use H.323 version 2 Registration, Admission, and Status (RAS), you do not specify an IP address using the **session target** command. Instead, you will use **session target ras**.

Both POTS and voice network dial peers are needed to establish voice connections over a packet network.

Dial-Peer Configuration Example

This diagram shows a dial-peer configuration.



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

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

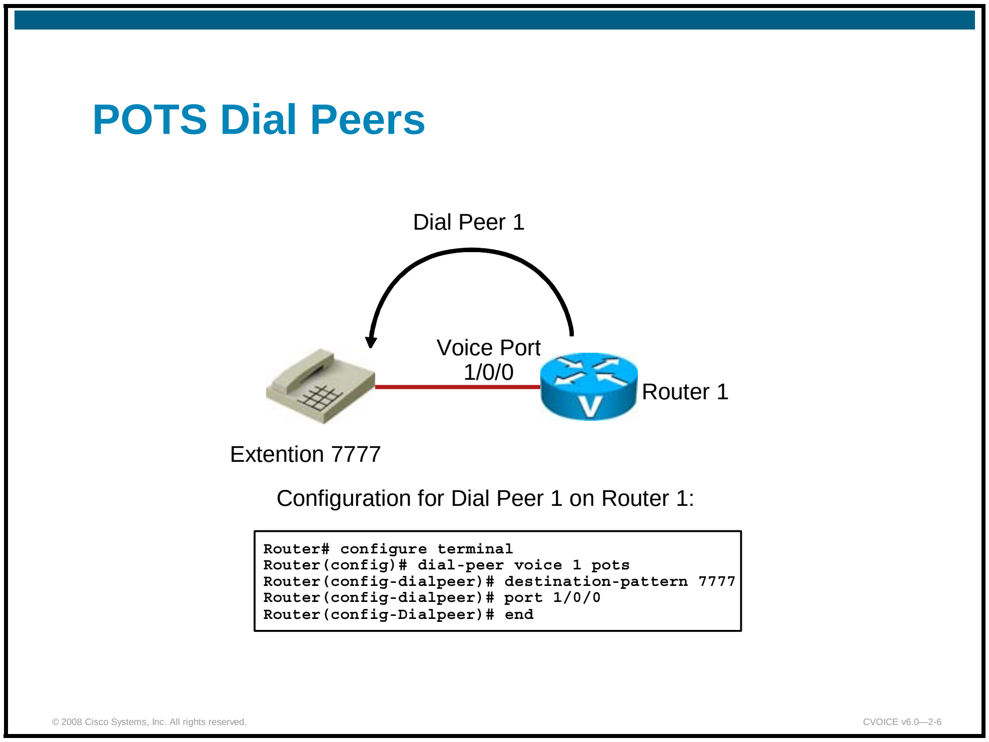
Complete these steps to place a VoIP call.

Step 1 Configure a compatible dial peer on the source router that specifies the recipient destination address.

Step 2 Configure a POTS dial peer on the recipient router that specifies which voice port the router uses to forward the voice call.

Configuring POTS Dial Peers

This topic describes how to configure POTS dial peers.



POTS Dial Peers

Configuration for Dial Peer 1 on Router 1:

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

Before the configuration of Cisco IOS dial peers can begin, the network administrator 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. The diagram in the figure illustrates proper POTS dial-peer configuration on a Cisco voice-enabled router.

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.

Complete these steps to configure POTS dial peers.

Step 1 Configure a POTS dial peer at each router or gateway where edge telephony devices connect to the network.

```
router(config)# dial-peer voice 1 pots
```

The **dial-peer voice 1 pots** command notifies the router that dial peer 1 is a POTS dial peer with a tag of 1.

Step 2 Configure the telephone number.

```
router(config-dial-peer)# destination-pattern 7777
```

The **destination-pattern 7777** command notifies the router that the attached telephony device terminates calls destined for telephone number 7777.

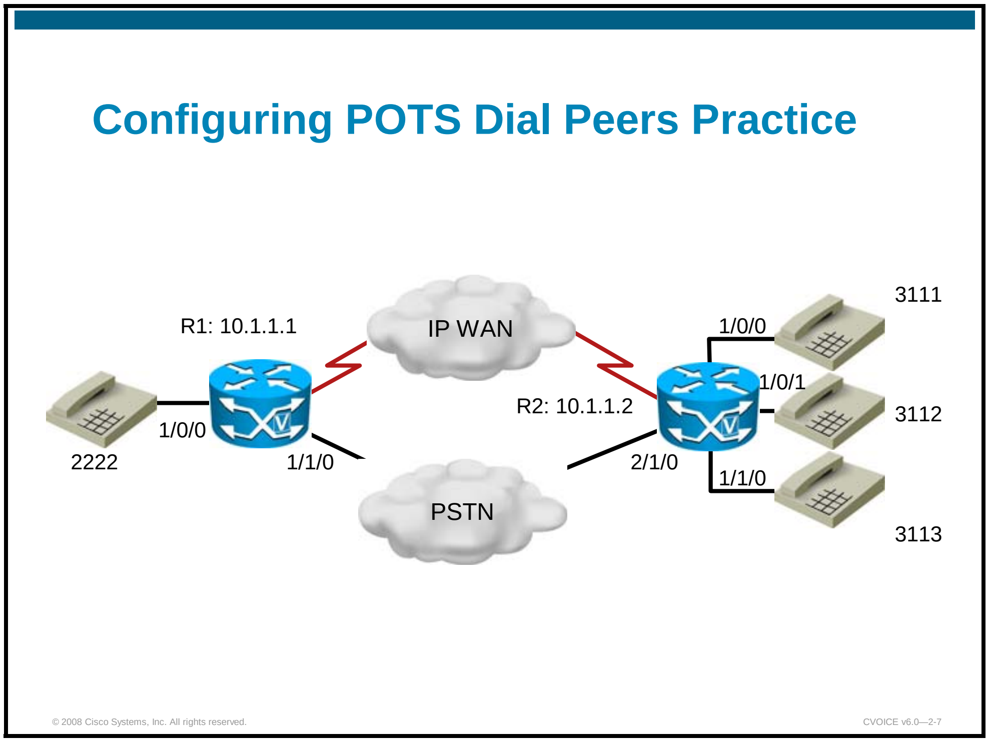
Step 3 Specify the physical voice port that the POTS telephone is connected to.

```
router(config-dial-peer)# port 1/0/0
```

The **port 1/0/0** command notifies the router that the telephony device is plugged into module 1, voice interface card (VIC) slot 0, and voice port 0.

POTS Dial-Peer Configuration Practice

This page can be used to practice dial peer configuration.



Configuring POTS Dial Peers Practice

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-7

Assume that there is a data center at the R1 site and executive offices at the R2 site. Using the diagram, create basic POTS dial peers on R1 and R2 for the four telephones shown.

R1 POTS

____

____

____

R2 POTS

____

____

____

____

____

____

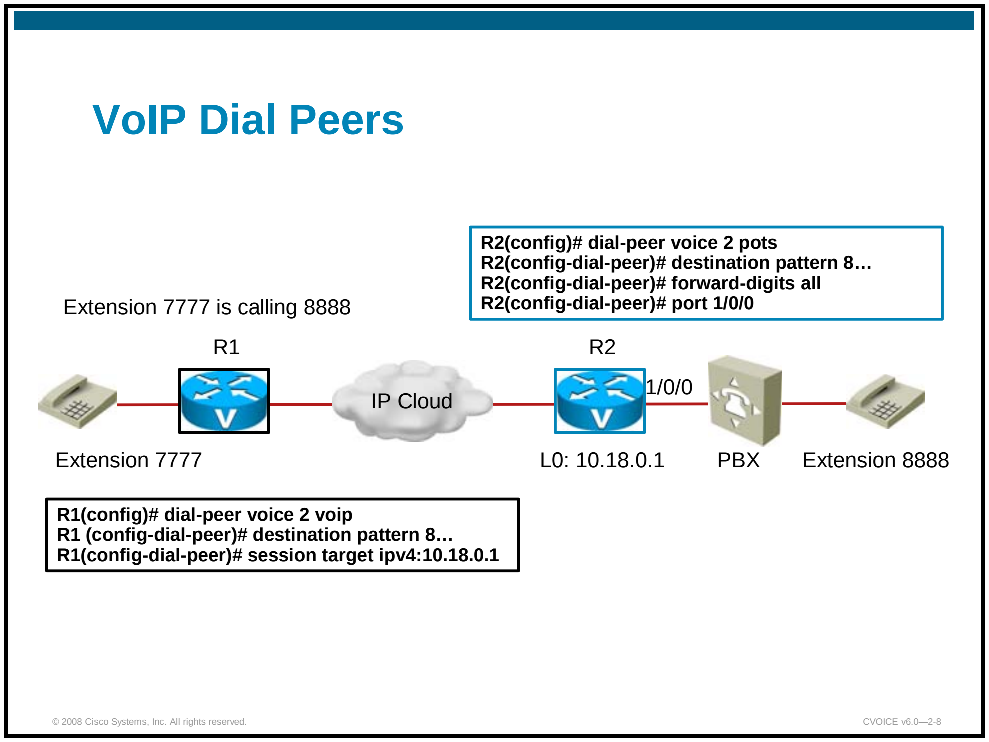
____

____

____

Configuring VoIP Dial Peers

This topic describes how to configure VoIP dial peers.



VoIP Dial Peers

```
R2(config)# dial-peer voice 2 pots
R2(config-dial-peer)# destination pattern 8…
R2(config-dial-peer)# forward-digits all
R2(config-dial-peer)# port 1/0/0
```

```
R1(config)# dial-peer voice 2 voip
R1 (config-dial-peer)# destination pattern 8…
R1(config-dial-peer)# session target ipv4:10.18.0.1
```

The administrator must know how to identify the far-end voice-enabled device that will terminate the call. In a small network environment, the device may be the IP address of the remote device. In a large environment, identifying the device may mean pointing to a Cisco Unified Communications Manager or gatekeeper for address resolution and Call Admission Control (CAC) to complete the call. The diagram in the figure illustrates the proper VoIP dial-peer configuration on a Cisco voice-enabled router.

Complete these steps to configure VoIP dial peers.

Configure the path across the network for voice data on R1.

Step 1 Specify the dial peer as a VoIP dial peer.

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 dial peer is specified as a VoIP dial peer, which alerts the router that it must process a call according to the various dial-peer parameters. The dial peer must then package it as an IP packet for transport across the network. Specified parameters may include the codec that is used for compression (VAD, for example), or marking the packet for priority service.

Step 2 Use the **destination-pattern** command to configure a range of numbers that are reachable by the remote router or gateway.

The **destination-pattern 8…** command notifies the router that this dial peer defines an IP voice path across the network for telephone numbers 8000 to 8999.

Note The **destination-pattern** command configured for this dial peer is typically a range of numbers that are reachable via the remote router or gateway.

Step 3 Use the **session target** command to specify an IP address of the terminating router or gateway.

The **session target ipv4:10.18.0.1** command defines the IP address of the router that is connected to the remote telephony device.

Because this dial peer points to a device across the network, the router needs a destination IP address to put in the IP packet. The **session target** command allows the administrator to specify either an IP address of the terminating router or gateway or of another device. For example, a gatekeeper or Cisco Unified Communications Manager may return an IP address of that remote terminating device.

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

Configure the outbound dial peer on R2 to route calls to the remote PBX.

Step 4 Specify the dial peer as a POTS dial peer.

The **dial-peer voice 2 POTS** command notifies the router that dial peer 2 is a POTS dial peer with a tag of 2.

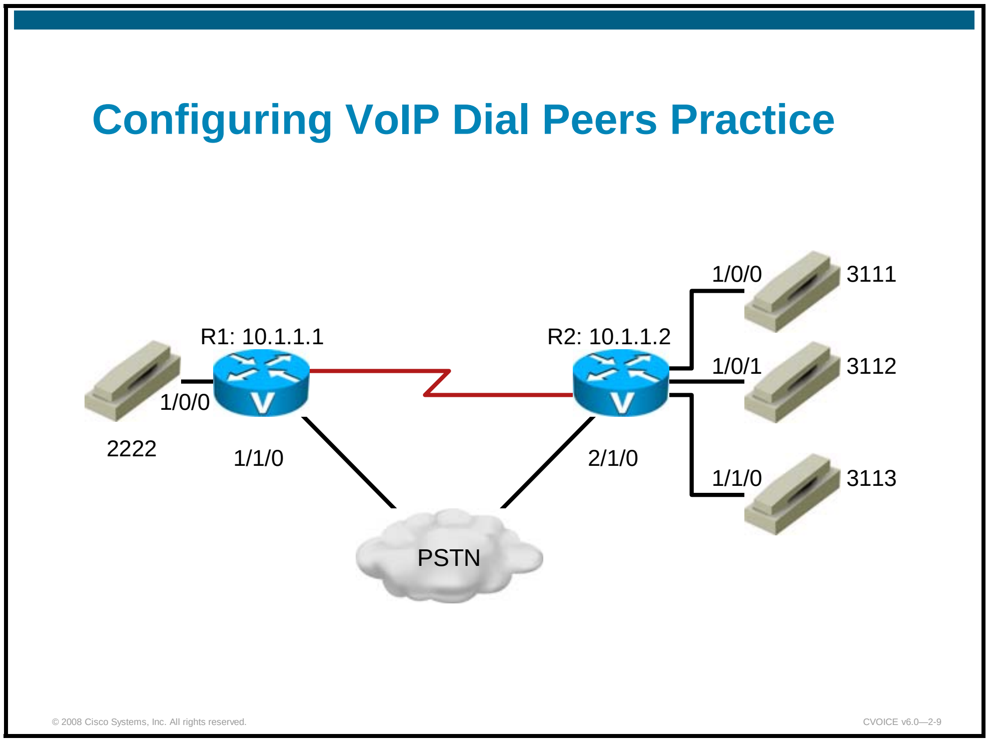
Step 5 Use the **destination-pattern** command to configure a range of numbers reachable by the router or gateway.

The **destination-pattern 8…** command notifies the router that this dial peer defines an POTS dial peer for a range of telephone number from 8000 to 8999.

Step 6 Use the **port** command to route calls to the PBX.

VoIP Dial-Peer Configuration Practice

This page can be used to practice dial-peer configuration.



Configuring VoIP Dial Peers Practice

© 2008 Cisco Systems, Inc. All rights reserved.

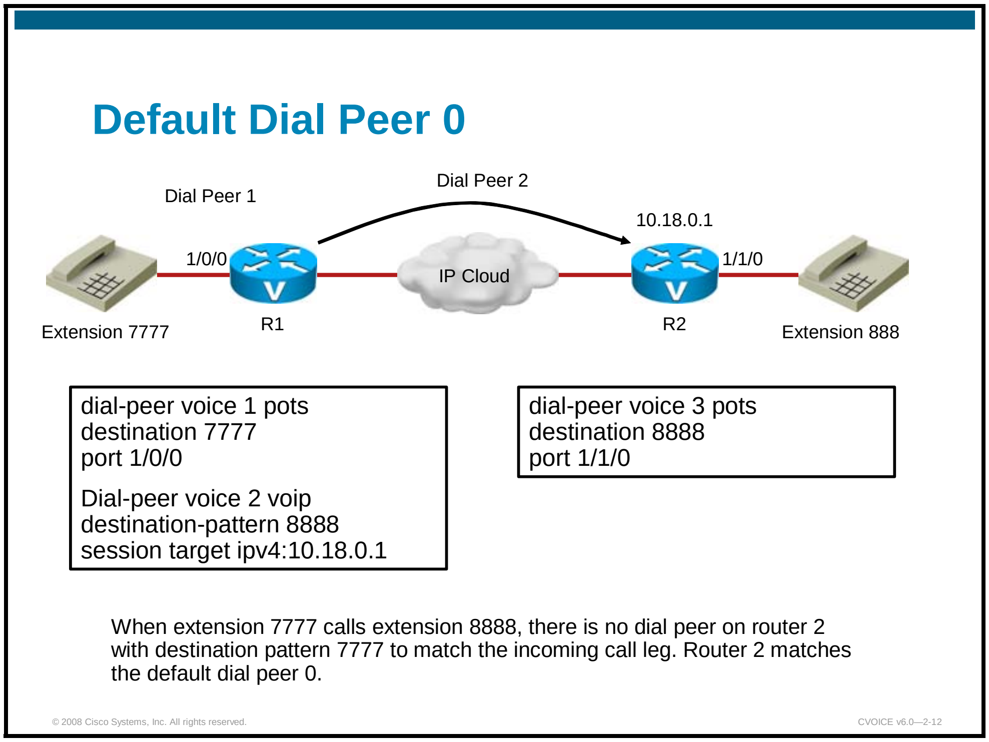
CVOICE v6.0—2-9

Using the diagram, create basic VoIP dial peers on R1 and R2 for the two gateways shown.

R1 VoIP	**R2 VoIP**
______________________	______________________
______________________	______________________
______________________	______________________

Default Dial Peer

This topic describes the default dial peer.



Default Dial Peer 0

```
dial-peer voice 1 pots
destination 7777
port 1/0/0

Dial-peer voice 2 voip
destination-pattern 8888
session target ipv4:10.18.0.1
```

```
dial-peer voice 3 pots
destination 8888
port 1/1/0
```

When extension 7777 calls extension 8888, there is no dial peer on router 2 with destination pattern 7777 to match the incoming call leg. Router 2 matches the default dial peer 0.

CVOICE v6.0—2-12

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.

Use of Default Dial Peer 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 toward router 1. Therefore, there is no dial peer on router 2 that will match the calling number of extension 7777 on the inbound call leg. If no incoming dial peer matches the calling number, the inbound call leg automatically matches to a default dial peer (POTS or VoIP).

Dial peer 0 for inbound VoIP peers has this configuration:

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

Dial peer 0 for inbound POTS peers has this configuration:

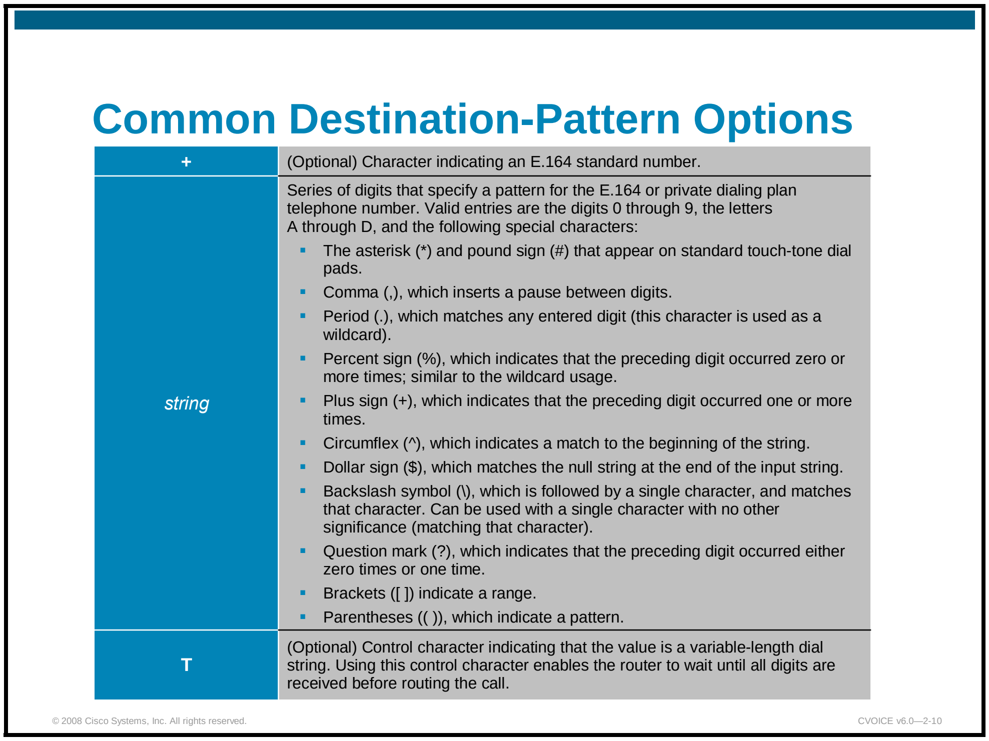
- **no ivr application**

You cannot change the default configuration for dial peer 0. Default dial peer 0 fails to negotiate nondefault capabilities or services. When the default dial peer is matched on a VoIP call, the call leg that is set up in the inbound direction uses any supported codec for voice compression that is based on the requested codec capability coming from the source router. When a default dial peer is matched, the voice path in one direction may have different parameters than the voice in the return direction. This difference in voice path parameters may cause one side of the connection to report good quality voice while the other side reports poor quality voice. For example, the outbound dial peer has VAD disabled, but the inbound call leg is matched against the default dial peer, which has VAD enabled. VAD would be on in one direction and off in the return direction.

When the default dial peer is matched on an inbound POTS call leg, there is no default IVR application with the port. As a result, the user gets a dial tone and proceeds with dialed digits.

Configuring Destination-Pattern Options

This topic describes how to use destination-pattern options to associate a telephone number with a given dial peer.



Common Destination-Pattern Options

+	(Optional) Character indicating an E.164 standard number.
string	Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and the following special characters: ▪ The asterisk (*) and pound sign (#) that appear on standard touch-tone dial pads. ▪ Comma (,), which inserts a pause between digits. ▪ Period (.), which matches any entered digit (this character is used as a wildcard). ▪ Percent sign (%), which indicates that the preceding digit occurred zero or more times; similar to the wildcard usage. ▪ Plus sign (+), which indicates that the preceding digit occurred one or more times. ▪ Circumflex (^), which indicates a match to the beginning of the string. ▪ Dollar sign ($), which matches the null string at the end of the input string. ▪ Backslash symbol (\), which is followed by a single character, and matches that character. Can be used with a single character with no other significance (matching that character). ▪ Question mark (?), which indicates that the preceding digit occurred either zero times or one time. ▪ Brackets ([ ]) indicate a range. ▪ Parentheses (( )), which indicate a pattern.
T	(Optional) Control character indicating that the value is a variable-length dial string. Using this control character enables the router to wait until all digits are received before routing the call.

CVOICE v6.0—2-10

The destination pattern you configure is used to match dialed digits to a dial peer. The dial peer is then used to complete the call.

When a router receives voice data, it compares the called number (the full E.164 telephone number) in the packet header with the number that is configured as the destination pattern for the voice telephony peer. It also determines the dialed digits that the router collects and forwards to the remote telephony interface, such as a PBX, Cisco Unified Communications Manager, or the PSTN.

Note	In the case of POTS dial peers, the router strips out the left-justified numbers that explicitly match the destination pattern. If you have configured a prefix, the prefix is appended to the front of the remaining numbers, creating a dial string, which the router then dials. If all numbers in the destination pattern are stripped out, the user receives a dial tone.

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, or it can point to a range of numbers defined in a variety of ways.

To specify either the prefix or the full E.164 telephone number to be used for a dial peer, use the **destination-pattern** command in dial peer configuration mode.

```
destination-pattern [+] string [T]
```

Destination-pattern options include those listed here:

- **Plus sign (+):** This is an optional character that indicates an E.164 standard number. E.164 is the ITU-T recommendation for the international public telecommunication numbering plan. The plus sign in front of a destination-pattern string specifies that the string must conform to E.164.
- ***string:*** This is a series of digits specifying the E.164 or private dial plan telephone number. The examples that follow show the use of special characters that are often found in destination-pattern strings:
  - An asterisk (*) and pound sign (#) appear on standard touch-tone dial pads. These characters may need to be used when passing a call to an automated application that requires these characters to signal the use of a special feature. For example, when a user calls an interactive voice response (IVR) system that requires a code for access, the number dialed might be "5551212888#", which would initially dial the telephone number "5551212" and input a code of "888" followed by the pound key to terminate the IVR input query.
  - A comma (,) inserts a 1-second pause between digits. The comma can be used, for example, where a "9" is dialed to signal a PBX that the call should be processed by the PSTN. The "9" is followed by a comma to give the PBX time to open a call path to the PSTN, after which the remaining digits will be played out. An example of this string is "9,5551212".
  - A period (.) matches any single entered digit from 0 to 9, and is used as a wildcard. The wildcard can be used to specify a group of numbers that may be accessible via a single destination router, gateway, PBX, or Cisco Unified Communications Manager. A pattern of "200." allows for 10 uniquely addressed devices, while a pattern of "20.." can point to 100 devices. If one site has the numbers 2000 through 2049, and another site has the numbers 2050 through 2099, the bracket notation would be more efficient.
  - Brackets ([ ]) indicate a range. A range is a sequence of characters that are enclosed in the brackets. Only single numeric characters from 0 to 9 are allowed in the range. In the previous example, the bracket notation could be used to specify exactly which range of numbers is accessible through each dial peer. For example, the first site pattern would be "20[0–4].", and the second site pattern would be "20[5–9].". Note that in both cases, a period is used in the last digit position to represent any single digit from 0 to 9. The bracket notation offers much more flexibility in how numbers can be assigned.
- **T:** This is an optional control character indicating that the destination-pattern value is a variable-length dial string. In this case, the system does not match the dialed numbers until the interdigit timeout value has expired. In cases where callers may be dialing local, national, or international numbers, the destination pattern must provide for a variable-length dial plan. If a particular voice gateway has access to the PSTN for local calls and access to a transatlantic connection for international calls, calls being routed to that gateway will have a varying number of dialed digits. A single dial peer with a destination pattern of ".T" could support the different call types. The **interdigit timeout** command determines when a string of dialed digits is complete. The router continues to collect digits until there is an interdigit pause longer than the configured value. 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.

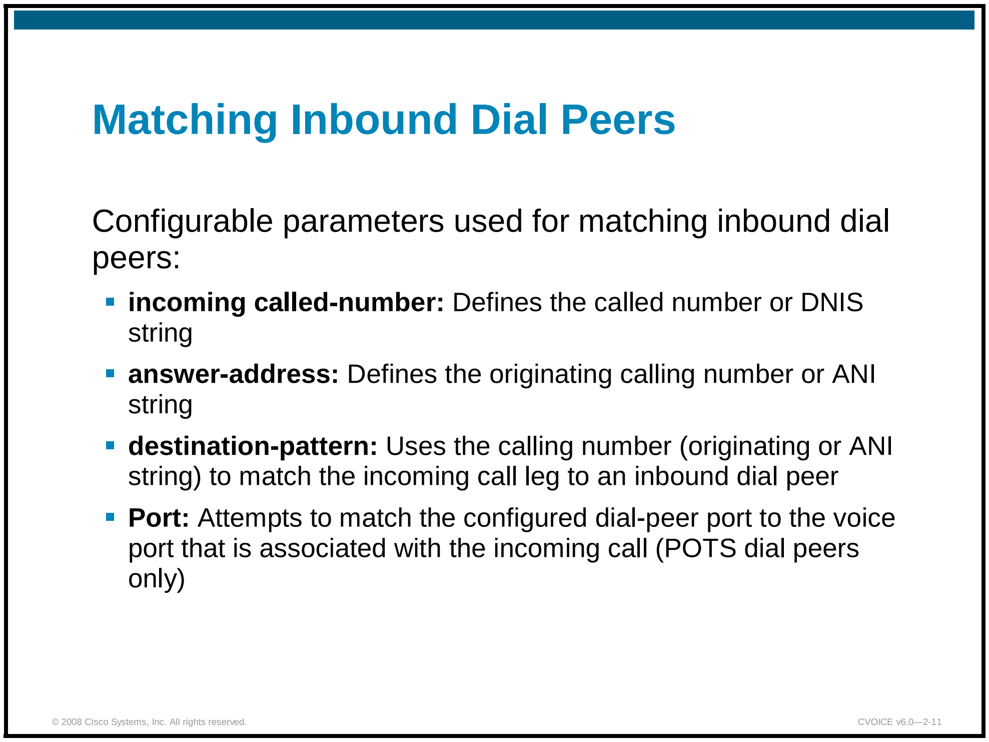
Matching Destination Patterns Example

Destination-Pattern Options

Destination Pattern	Matching Telephone Numbers
5550124	This destination pattern matches one telephone number exactly, 5550124. This destination pattern is typically used when there is a single device, such as a telephone or fax, connected to a voice port.
55501[1-3].	This destination pattern matches a seven-digit telephone number where the first five digits are 55501, the sixth digit can be a 1, 2, or 3, and the last digit can be any valid digit. This destination pattern is used when telephone number ranges are assigned to specific sites. In this example, the destination pattern is used in a small site that does not need more than 30 numbers assigned.
.T	This destination pattern matches any telephone number that has at least 1 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, for local, national, and international calls. It can also be used as a default destination pattern so that any calls that do not match a more specific pattern will match this pattern and can be directed to an operator.

Matching Inbound Dial Peers

This topic describes how the router matches inbound dial peers.



Matching Inbound Dial Peers

Configurable parameters used for matching inbound dial peers:

- **incoming called-number:** Defines the called number or DNIS string
- **answer-address:** Defines the originating calling number or ANI string
- **destination-pattern:** Uses the calling number (originating or ANI string) to match the incoming call leg to an inbound dial peer
- **Port:** Attempts to match the configured dial-peer port to the voice port that is associated with the incoming call (POTS dial peers only)

CVOICE v6.0—2-11

When you are determining how inbound dial peers are matched on a router, it is important to note whether the inbound call leg is matched to a POTS or VoIP dial peer. Matching occurs in the following manner:

- Inbound POTS dial peers are associated with the incoming POTS call legs of the originating router or gateway.
- Inbound VoIP dial peers are associated with the incoming VoIP call legs of the terminating router or gateway.

Three information elements sent in the call setup message are matched against four configurable dial-peer command attributes. Those three elements are listed in the table.

Call Setup Information Elements

Call Setup Element	Description
Called number Dialed Number Identification Service (DNIS)	This is the call destination dial string, and it is derived from the ISDN setup message or channel associated signaling the DNIS.
Calling number Automatic Number Identification (ANI)	This is a number string that represents the origin, and it is derived from the ISDN setup message or channel associated signaling (CAS) ANI. The ANI is also referred to as the calling line ID (CLID).
Voice port	This represents the POTS physical voice port.

When the Cisco IOS router or gateway receives a call setup request, it looks for a dial-peer match for the incoming call. This is not digit-by-digit matching. Instead, the router uses the full digit string received in the setup request for matching against the configured dial peers.

The router or gateway matches call setup element parameters in the order listed here.

1. The router or gateway attempts to match the called number of the call setup request with the configured **incoming called-number** parameter of each dial peer.
2. If a match is not found, the router or gateway attempts to match the calling number of the call setup request with the **answer-address parameter** of each dial peer.
3. If a match is not found, the router or gateway attempts to match the calling number of the call setup request to the **destination-pattern** parameter of each dial peer.
4. The voice port uses the voice port number associated with the incoming call setup request to match the inbound call leg to the configured dial peer **port** parameter.
5. If multiple dial peers have the same port configured, the router or gateway matches the first dial peer added to the configuration.
6. If a match is not found in the previous steps, the default is dial peer 0.

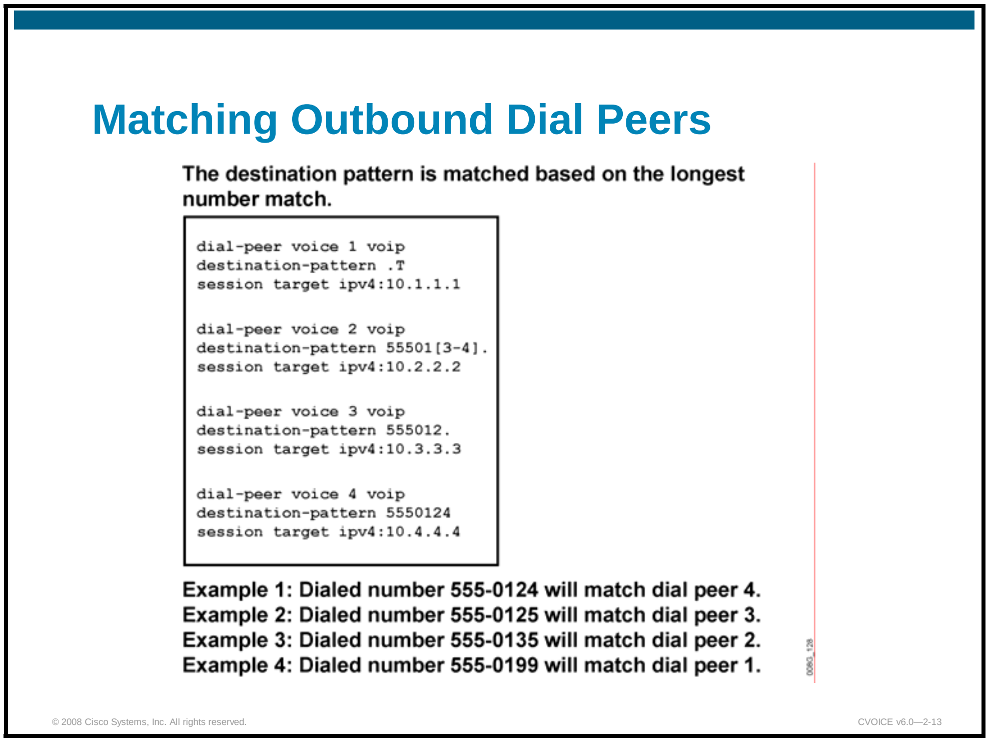
Because call setups always include DNIS information, it is recommended that you use the **incoming called-number** command for inbound dial-peer matching. Configuring **incoming called-number** command is useful for a company that has a central call center that provides support for a number of different products. Purchasers of each product get a unique toll-free number to call for support. All support calls are routed to the same trunk group destined for the call center. When a call comes in, the computer telephony system uses the DNIS to flash the appropriate message on the computer screen of the agent to whom the call is routed. The agent will then know how to customize the greeting when answering the call.

The calling number ANI with **answer-address** command is useful when you want to match calls based on the originating calling number. For example, when a company has international customers who require foreign-language-speaking agents to answer the call, the call can be routed to the appropriate agent based on the country of call origin.

You must use the calling number ANI with the **destination-pattern** command when the dial peers are set up for two-way calling. In a corporate environment, the head office and the remote sites must be connected. As long as each site has a VoIP dial peer configured to point to each site, inbound calls from the remote site will match against that dial peer.

Matching Outbound Dial Peers

This topic describes how the router matches outbound dial peers.



Matching Outbound Dial Peers

The destination pattern is matched based on the longest number match.

```
dial-peer voice 1 voip
destination-pattern .T
session target ipv4:10.1.1.1

dial-peer voice 2 voip
destination-pattern 55501[3-4].
session target ipv4:10.2.2.2

dial-peer voice 3 voip
destination-pattern 555012.
session target ipv4:10.3.3.3

dial-peer voice 4 voip
destination-pattern 5550124
session target ipv4:10.4.4.4
```

Example 1: Dialed number 555-0124 will match dial peer 4.
Example 2: Dialed number 555-0125 will match dial peer 3.
Example 3: Dialed number 555-0135 will match dial peer 2.
Example 4: Dialed number 555-0199 will match dial peer 1.

CVOICE v6.0—2-13

Outbound dial-peer matching is completed on a digit-by-digit basis. Therefore, the router or gateway checks for dial-peer matches after receiving each digit and then routes the call when a full match is made.

The router or gateway matches outbound dial peers in the order listed as follows:

1. The router or gateway uses the dial peer **destination-pattern** command to determine which dial-peer will be used to route the call.

2. The dial-peer configuration will then determine where to forward the call using one of the following configuration commands:

   — POTS dial peers use the **port** command.

   — VoIP dial peers use the **session target** command.

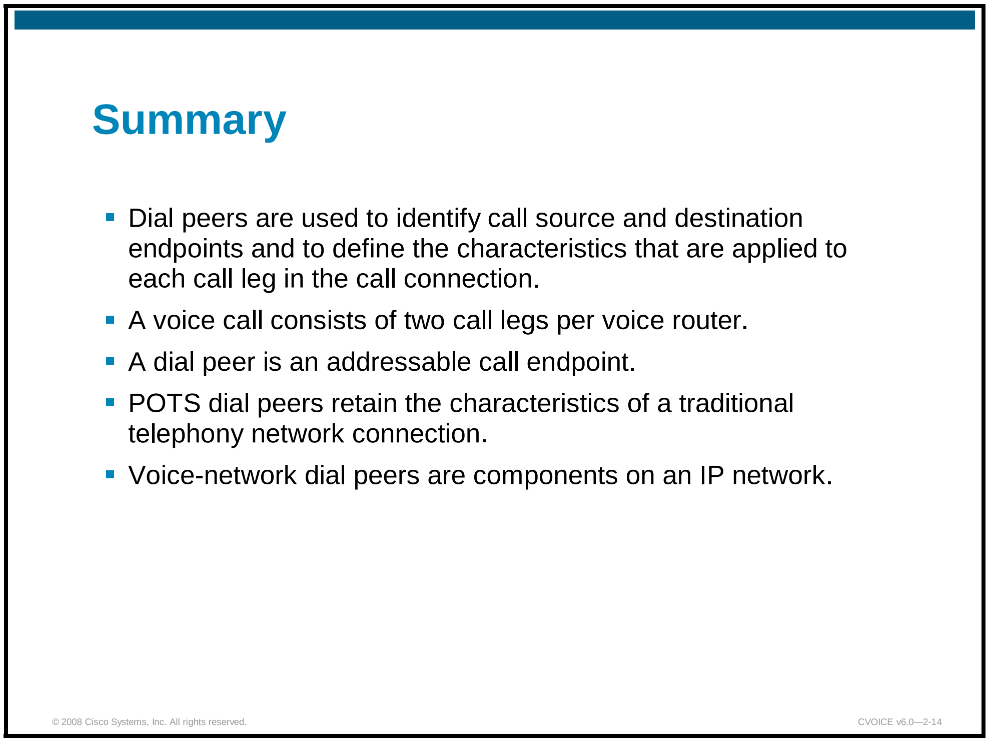
3. Use the **show dialplan number** *string* command to determine which dial peer is matched to a specific dialed string. This command displays all matching dial peers in the order that they are used.

Matching Outbound Dial Peers Example

In the diagram above, dial peer 1 matches any digit string that does not match the other dial peers more specifically. Dial peer 2 matches any seven-digit number in the 30 and 40 range of numbers starting with 55501. Dial peer 3 matches any seven-digit number in the 20 range of numbers starting with 555012. Dial peer 4 matches the specific number 5550124 only. When the number 5550124 is dialed, dial peers 1, 3, and 4 all match that number, but dial peer 4 places that call because it contains the most specific destination pattern.

Summary

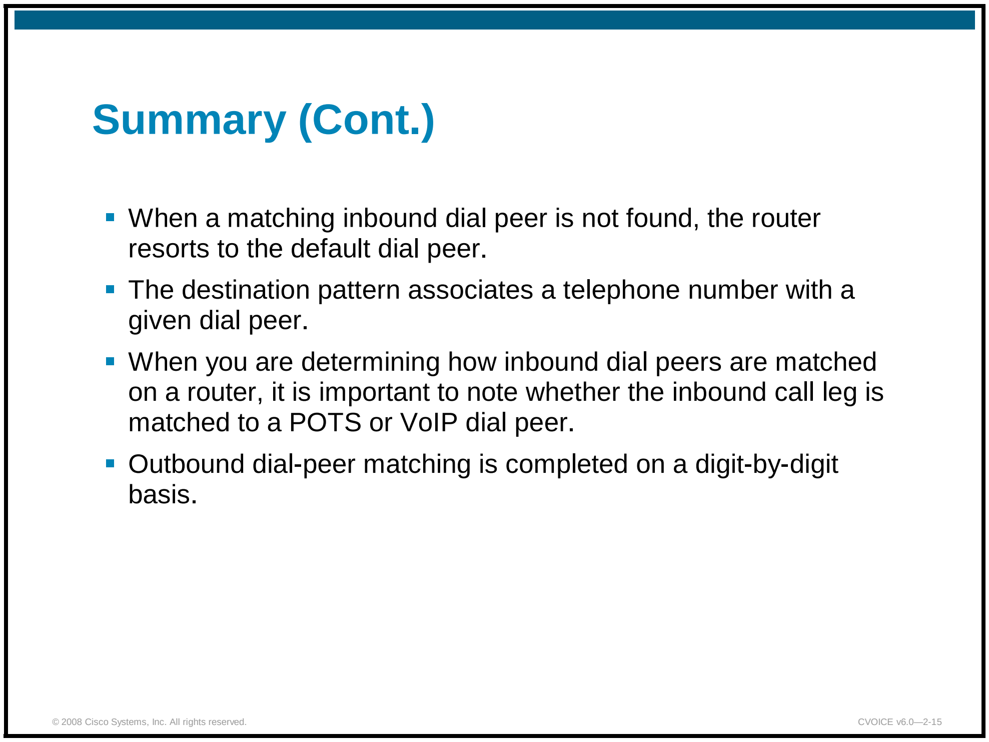
This topic summarizes the key points that were discussed in this lesson.



Summary

- Dial peers are used to identify call source and destination endpoints and to define the characteristics that are applied to each call leg in the call connection.
- A voice call consists of two call legs per voice router.
- A dial peer is an addressable call endpoint.
- POTS dial peers retain the characteristics of a traditional telephony network connection.
- Voice-network dial peers are components on an IP network.

CVOICE v6.0—2-14



Summary (Cont.)

- When a matching inbound dial peer is not found, the router resorts to the default dial peer.
- The destination pattern associates a telephone number with a given dial peer.
- When you are 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.
- Outbound dial-peer matching is completed on a digit-by-digit basis.

CVOICE v6.0—2-15

Lesson Self-Check

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

Q1) How many inbound call legs are associated with an established end-to-end call?

Relates to: Dial Peers and Call Legs

A) one
B) two
C) three
D) four

Q2) Which dial peers should you configure to complete an end-to-end call?

Relates to: Dial Peers and Call Legs

A) the inbound dial peers only
B) the outbound dial peers only
C) one inbound dial peer and one outbound dial peer
D) all four dial peers

Q3) Arrange the steps in the call-setup process in the correct order.

Relates to: End-to-End Calls

_____ 1. Router 2 creates the inbound voice network call leg and assigns it a call ID.

_____ 2. The POTS call arrives at router 1, and an inbound POTS dial peer is matched.

_____ 3. Router 1 creates an outbound voice network call leg and assigns it a call ID.

_____ 4. Router 1 creates an inbound POTS call leg and assigns it a call ID.

_____ 5. The voice network call request arrives at router 2 and an inbound voice network dial peer is matched.

_____ 6. Router 2 creates an outbound POTS call leg and assigns it a call ID.

_____ 7. Router 2 uses the dialed string to match an outbound POTS dial peer.

_____ 8. At this point, both router 1 and router 2 negotiate voice network capabilities and applications, if required.

_____ 9. Router 1 uses the dialed string to match an outbound voice network dial peer.

Q4) What is the role of the terminating router if the originating router requests nondefault voice capabilities?

Relates to: End-to-End Calls

A) The terminating router negotiates with the originating router until the default capabilities are accepted.
B) The terminating router reconfigures the ports to meet the requested capabilities.
C) The terminating router matches an inbound voice network dial peer that has the requested capabilities.
D) The terminating router terminates the call.

Q5) Which two functions are performed by a POTS dial peer? (Choose two.)

Relates to: Types of Dial Peers

A) providing an address for the edge network or device
B) providing a destination address for the edge device that is located across the network
C) routing the call across the network
D) identifying the specific voice port that connects the edge network or device
E) associating the destination address with the next-hop router or destination router, depending on the technology used

Q6) What do we call the address is that is configured on each dial peer?

Relates to: Types of Dial Peers

A) telephone number
B) number range
C) destination pattern
D) call endpoint

Q7) Which two parameters must be specified on a router that is connected to a telephone? (Choose two.)

Relates to: Configuring POTS Dial Peers

A) voice port
B) dial type
C) calling plan
D) telephone number
E) **ds0-group**

Q8) On which router or routers must you configure a POTS dial peer?

Relates to: Configuring POTS Dial Peers

A) one inbound router on the network
B) one outbound router on the network
C) one inbound and one outbound router on the network
D) each router where edge telephony devices connect to the network

Q9) Which command is used to specify the address of the terminating router or gateway?

Relates to: Configuring VoIP Dial Peers

A) **destination-port**
B) **destination-pattern**
C) **session target**
D) **destination address**
E) **dial-peer terminal**

Q10) Why should the loopback address be used in the **session target** command?

Relates to: Configuring VoIP Dial Peers

A) The call fails if the interface goes down.
B) The interface will never shut down.
C) The call will use an alternate path if the interface shuts down.
D) The call will never fail as long as the router is operating.

Q11) What does a plus (+) sign before the telephone number indicate?

Relates to: Configuring Destination-Pattern Options

A) The telephone number must conform to ITU-T Recommendation E.164.
B) The number is an extension of a telephone number.
C) An additional digit must be dialed before the telephone number.
D) The telephone number can vary in length.

Q12) Which special character in a destination-pattern string is used as a wildcard?

Relates to: Configuring Destination-Pattern Options

A) asterisk (*)
B) pound sign (#)
C) comma (,)
D) period (.)
E) brackets ([])

Q13) What happens when no matching dial peer is found for an outbound call?

Relates to: Default Dial Peer

A) The default dial peer is used.
B) Dial peer 0 is used.
C) The POTS dial peer is used.
D) The call is dropped.

Q14) Which four commands are used to configure the default dial-peer for inbound VoIP dial-peers? (Choose four.)

Relates to: Default Dial Peer

A) **any codec**
B) **no ivr application**
C) **vad enabled**
D) **no rsvp support**
E) **ip precedence 0**
F) **destination-pattern .T**
G) **default voice port**

Q15) Which parameter is configured only for POTS dial peers?

Relates to: Matching Inbound Dial Peers

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

Q16) What is the sequence that the router uses when it is matching the called number in the call setup request to a dial-peer attribute?

Relates to: Matching Inbound Dial Peers

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

Q17) Match the dialed number to its most specific dial-peer.

Relates to: Matching Outbound Dial Peers

A) 5551234
B) 5553000
C) 5553216
D) 5554123

_____ 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

Q18) When the router finds a matching outbound VoIP dial peer, which command determines where to forward the call?

Relates to: Matching Outbound Dial Peers

A) **destination-pattern**
B) **port**
C) **session target**
D) **dialplan number**

Lesson Self-Check Answer Key

Q1) B

Q2) D

Q3)

Step 1 The POTS call arrives at router 1, and an inbound POTS dial peer is matched. (2.)

Step 2 Router 1 creates an inbound POTS call leg and assigns it a call ID. (4.)

Step 3 Router 1 uses the dialed string to match an outbound voice network dial peer. (9.)

Step 4 Router 1 creates an outbound voice network call leg and assigns it a call ID. (3.)

Step 5 The voice network call request arrives at router 2 and an inbound voice network dial peer is matched. (5.)

Step 6 Router 2 creates the inbound voice network call leg and assigns it a call ID. (1.)

Step 7 At this point, both router 1 and router 2 negotiate voice network capabilities and applications, if required. (8.)

Step 8 Router 2 uses the dialed string to match an outbound POTS dial peer. (7.)

Step 9 Router 2 creates an outbound POTS call leg and assigns it a call ID. (6.)

Q4) C

Q5) A, D

Q6) C

Q7) A, D

Q8) D

Q9) C

Q10) B

Q11) A

Q12) D

Q13) D

Q14) A, C, D, E

Q15) D

Q16) 1. **incoming called-number**
2. **answer-address**
3. **destination-pattern**
4. **port**

Q17) 1-D, 2-A, 3-B, 4-C

Q18) C

Lesson 4

Configuring Digital Voice Ports

Overview

Digital trunks are used to connect to the public switched telephony network (PSTN), to a PBX, or to the WAN and are widely available worldwide. In some areas, channel associated signaling (CAS) trunks are the only connections available. BRI and PRI trunks are very common when a voice gateway is being connected to the PSTN. This lesson maps out the various digital interfaces and explains how to implement and verify digital trunks.

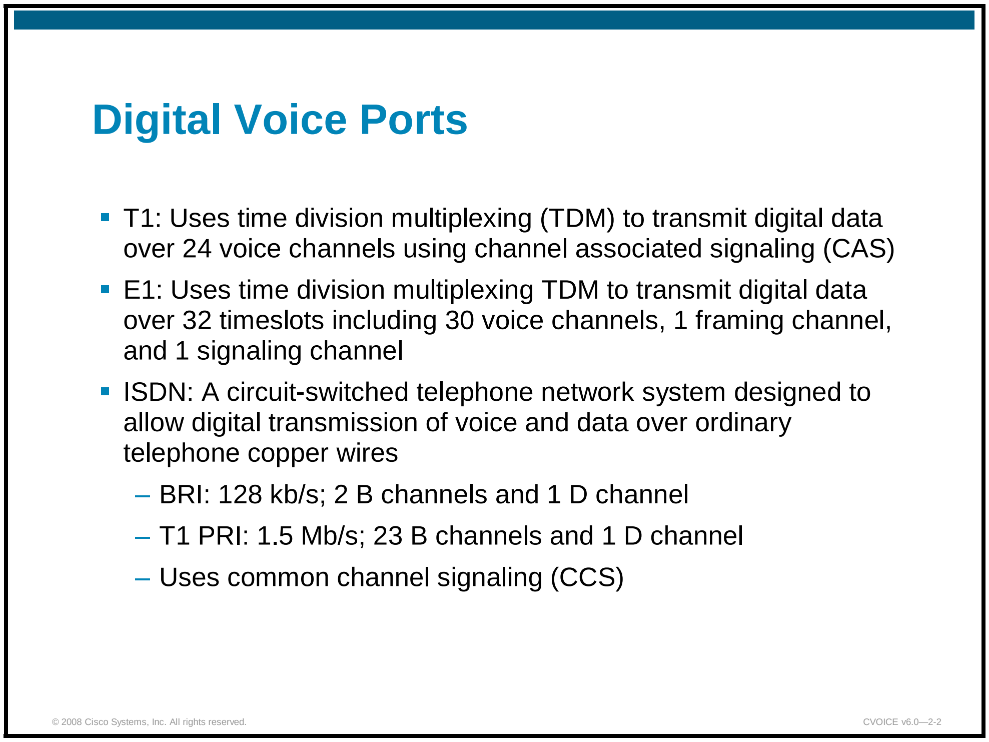
Objectives

Upon completing this lesson, you will be able to describe various digital interfaces and how to configure them as trunks. This ability includes being able to meet these objectives:

- Describe the types of digital voice ports
- Describe T1 CAS trunks and associated signaling
- Describe E1 R2 CAS trunks and associated signaling
- Describe ISDN
- Describe ISDN signaling
- Configure a T1 CAS trunk to the PSTN
- Configure an E1 CAS trunk to the PSTN
- Configure and verify BRI and PRI trunks to the PSTN
- Describe how to verify digital voice port connections

Digital Voice Ports

This topic describes the various types of digital voice ports.



Digital Voice Ports

- T1: Uses time division multiplexing (TDM) to transmit digital data over 24 voice channels using channel associated signaling (CAS)
- E1: Uses time division multiplexing TDM to transmit digital data over 32 timeslots including 30 voice channels, 1 framing channel, and 1 signaling channel
- ISDN: A circuit-switched telephone network system designed to allow digital transmission of voice and data over ordinary telephone copper wires
  - BRI: 128 kb/s; 2 B channels and 1 D channel
  - T1 PRI: 1.5 Mb/s; 23 B channels and 1 D channel
  - Uses common channel signaling (CCS)

CVOICE v6.0—2-2

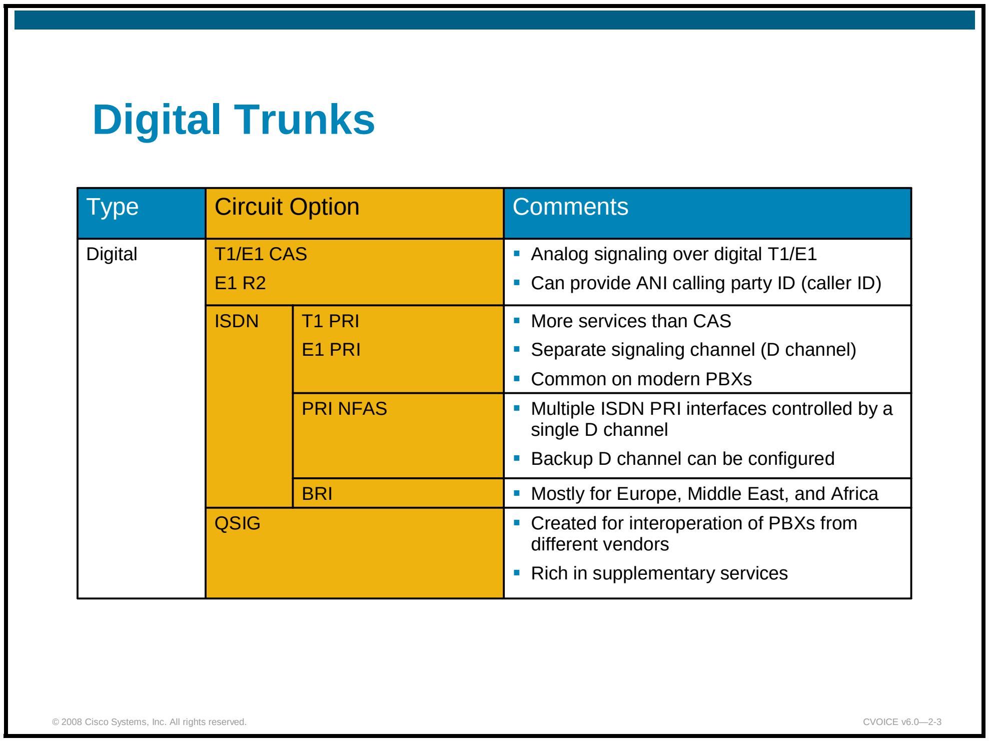
Digital voice ports are found at the intersection of a packet voice network and a digital, circuit-switched telephone network. The digital voice port interfaces that connect the router or access server to T1 or E1 lines pass voice data and signaling between the packet network and the circuit-switched network.

There are three types of digital voice circuits that are supported on Cisco voice gateways:

- **T1:** Uses time-division multiplexing (TDM) to transmit digital data over 24 voice channels using channel associated signaling (CAS)
- **E1:** Uses TDM to transmit digital data over 30 voice channels using either CAS or common channel signaling (CCS)
- **ISDN:** Is a circuit-switched telephone network system using CCS.
  - BRI; 2 bearer (B) channels and 1 data (D) channel
  - T1 PRI; 23 B channels and 1 D channel

Digital Trunks

This subtopic describes digital trunks and their associated signaling.



Digital Trunks

Type	Circuit Option		Comments
Digital	T1/E1 CAS E1 R2		▪ Analog signaling over digital T1/E1 ▪ Can provide ANI calling party ID (caller ID)
	ISDN	T1 PRI E1 PRI	▪ More services than CAS ▪ Separate signaling channel (D channel) ▪ Common on modern PBXs
		PRI NFAS	▪ Multiple ISDN PRI interfaces controlled by a single D channel ▪ Backup D channel can be configured
		BRI	▪ Mostly for Europe, Middle East, and Africa
	QSIG		▪ Created for interoperation of PBXs from different vendors ▪ Rich in supplementary services

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-3

Digital voice ports are used to interconnect gateways or PBX systems to other gateways, PBX systems, or the PSTN. A trunk is a single physical or logical interface that contains several physical interfaces and connects to a single destination. This figure gives an overview of the most common digital trunks.

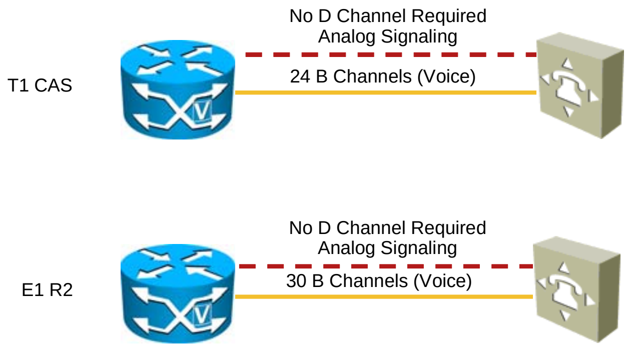
There are two aspects to consider when you are configuring signaling on digital lines: one aspect is the actual information about line and device states that is transmitted, and the second aspect is the method that is used to transmit the information on the digital lines.

The actual information about line and device states is communicated over digital lines using signaling methods that emulate the methods that are used in analog circuit-switched networks: Foreign Exchange Station (FXS), Foreign Exchange Office (FXO), and recEive and transMit (E&M).

For signaling to pass between a packet network and a circuit-switched network, both networks must use the same type of signaling. The voice ports on Cisco routers and access servers can be configured to match the signaling of most central offices (COs) and PBXs.

The table in the figure lists some of the common digital circuit options.

Digital Trunks (Cont.)



CVOICE v6.0—2-4

The T1, E1, or ISDN lines that connect a telephony network to the digital voice ports on a router or access server contain channels for voice calls; a T1 or ISDN PRI line contains 24 full-duplex channels or time slots, and an E1 line contains 30. The signal on each channel is transmitted at 64 kb/s, a standard known as digital service level 0 (DS0); the channels are known as DS0 channels. The **ds0-group** command creates a logical voice port (a DS0 group) from some or all of the DS0 channels, which allows you to address those channels easily, as a group, in voice port configuration commands.

The method that is used to transmit the information describes the way in which the emulated analog signaling is transmitted over digital lines.

Digital lines use two types of signaling:

- **CAS:** Takes place within the voice channel itself
- **CCS:** Sends signaling information down a dedicated channel

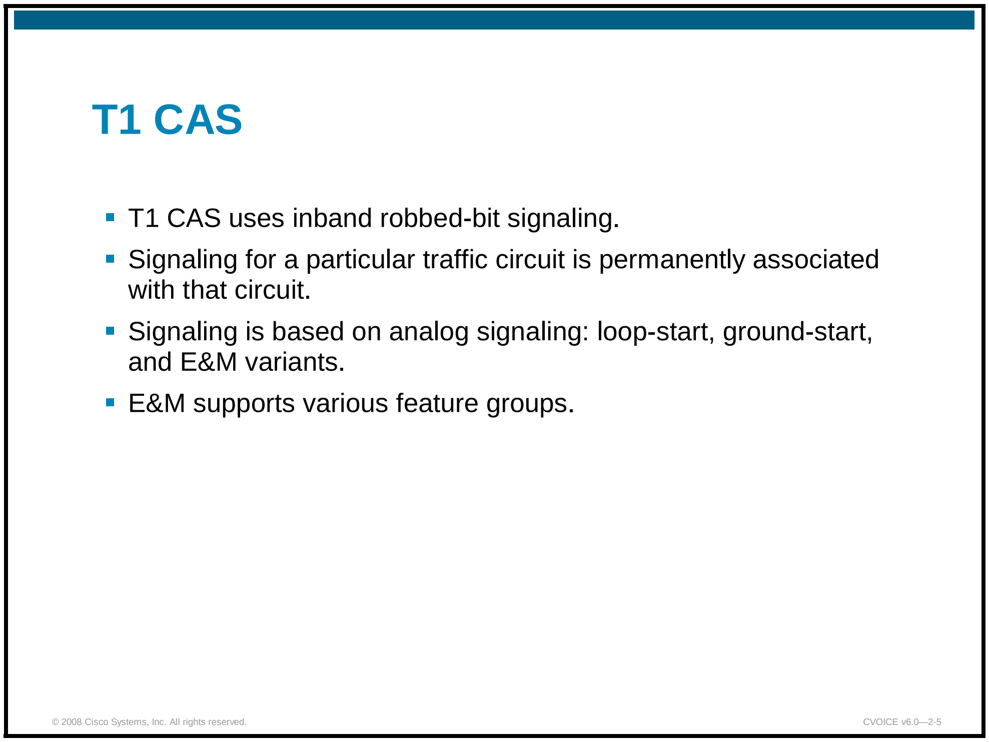
Two main types of digital trunks with CAS exist:

- **T1 CAS trunk:** This type of circuit allows analog signaling via a digital T1 circuit. There are many CAS variants that operate over analog and digital interfaces. A common digital interface that is used is T1 or E1 (European version), where each channel includes a dedicated signaling element (also called “robbed-bit signaling” on T1s). The type of signaling that is most commonly used with T1 CAS is E&M signaling. PRI is similar to ISDN except that it has an additional B channel available. In addition to setting up and tearing down calls, CAS provides the receipt and capture of Dialed Number Identification Service (DNIS) and Automatic Number Identification (ANI) information, which are used to support authentication and other functions. The main disadvantage of CAS signaling is its use of user bandwidth to perform these signaling functions.

- **E1 R2 trunk:** R2 signaling is a CAS system that was developed in the 1960s and is still in use today in Europe, Central and South America Australia, and Asia. R2 signaling exists in several country versions or variants in an international version called ITU-T R2. The R2 signaling specifications are contained in ITU-T Recommendations Q.400 through Q.490. R2 also provides ANI.

T1 CAS

This topic describes T1 CAS trunks and associated signaling.



T1 CAS

- T1 CAS uses inband robbed-bit signaling.
- Signaling for a particular traffic circuit is permanently associated with that circuit.
- Signaling is based on analog signaling: loop-start, ground-start, and E&M variants.
- E&M supports various feature groups.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-5

T1s have been around since the early voice networks. They were developed as a means of carrying multiple calls across one copper loop. Because the copper loop could carry much more bandwidth than the 4000 Hz that was required for voice transmission, T1s first used frequency-division multiplexing (FDM) to transmit 24 calls across a single copper loop. Currently, T1 circuits use TDM to transmit digital data (1s and 0s) instead of the old analog signals.

A single digital voice channel requires 64 kb/s of bandwidth. This is calculated using the following formula:

64 kb/s = 8000 samples/sec * 8 bits/sample = 64,000 b/s

This 64-kb/s voice channel is also known as DS0. With 24 voice channels at 64 kb/s per channel, a T1 represents 1.536 Mb/s of data. Add an additional 8 kb/s for framing, and the total speed of a T1 circuit equals 1.544 Mb/s.

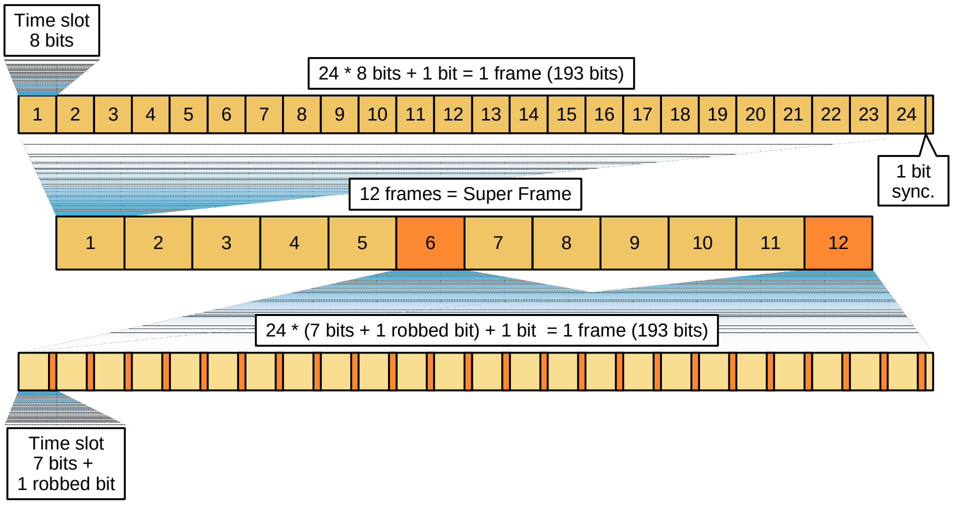
T1 CAS Signaling

T1 CAS uses a digital T1 circuit with in-band CAS. CAS is accomplished by using bits in the actual voice channel to transmit signaling information. CAS is sometimes called robbed-bit signaling because user bandwidth is robbed by the network for signaling. A bit is taken from every sixth frame of voice data to communicate on- or off-hook status, wink-start, ground-start, dialed digits, and other information about the call.

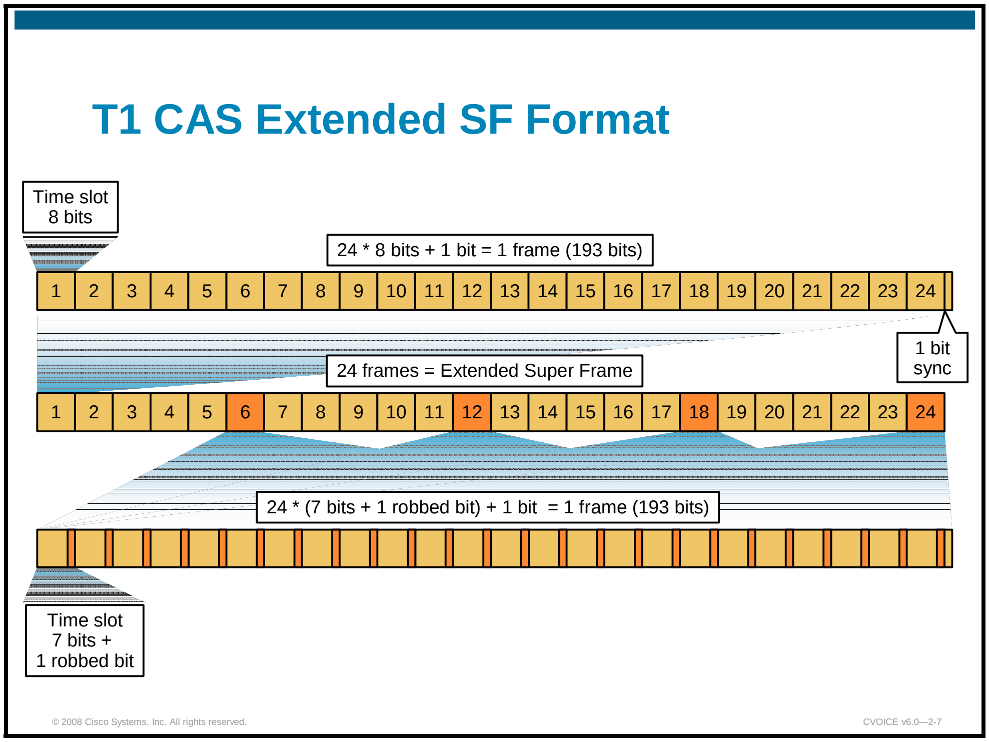
T1 CAS uses the same signaling types that are available for analog trunks: loop-start, ground-start, and E&M variants such as wink-start and immediate-start. There are also various feature groups that are available when you use E&M. Here are some common feature groups:

- **E&M Feature Group B (FGB):** Provides inbound and outbound DNIS, and inbound ANI (only on Cisco AS5300 Series Universal Access Servers, Cisco AS5400 Series Universal Gateways, and Cisco AS5800 Series Universal Gateways)
- **E&M Feature Group D (FGD):** Provides inbound and outbound DNIS, and inbound ANI
- **E&M FGD-Exchange Access North American (EANA):** Provides inbound and outbound DNIS, and outbound ANI

T1 CAS SF Format



This figure shows the CAS with the T1 Super Frame (SF) format. The top row of boxes represents a single T1 frame with 24 time slots of 8 bits each. An additional bit, used to synchronize the SF, is added at the end of each frame. A sequence of 12 T1 frames makes up one SF. CAS is implemented by robbed-bit signaling in frames 6 and 12 in this sequence. The bottom row of boxes represents T1 frames 6 and 12. The least significant bit of each voice channel is robbed, leaving 7 bits for voice data.

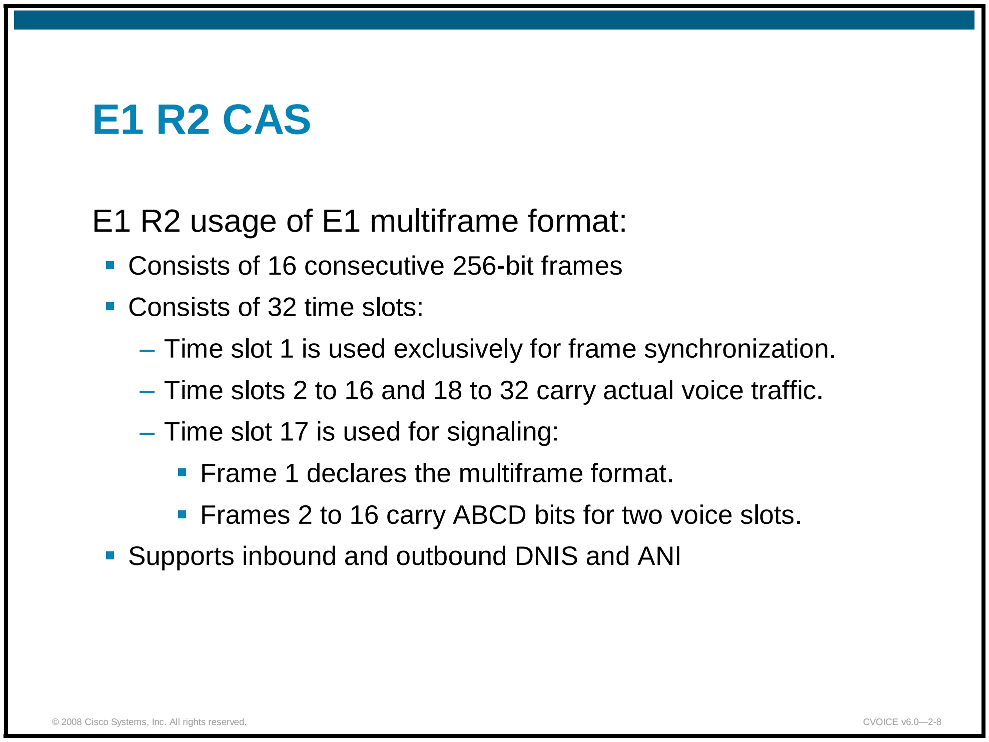


T1 CAS Extended SF Format

The Extended Super Frame (ESF) format was developed as an upgrade to SF and is now dominant in public and private networks. Both formats retain the basic frame structure of one framing bit followed by 192 data bits. However, ESF repurposes the use of the F bit. In ESF, of the total 8000 F bits that are used in T1, 2000 are used for framing, 2000 are used for cyclic redundancy 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).

E1 R2 CAS

This topic describes E1 R2 CAS trunks and associated signaling.



E1 R2 CAS

E1 R2 usage of E1 multiframe format:

- Consists of 16 consecutive 256-bit frames
- Consists of 32 time slots:
  - Time slot 1 is used exclusively for frame synchronization.
  - Time slots 2 to 16 and 18 to 32 carry actual voice traffic.
  - Time slot 17 is used for signaling:
    - Frame 1 declares the multiframe format.
    - Frames 2 to 16 carry ABCD bits for two voice slots.
- Supports inbound and outbound DNIS and ANI

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-8

An E1 circuit is similar to a T1 circuit. It is a TDM circuit that carries several DS0s in one connection. E1 circuits are widely used in Europe, Asia, and Central and South America.

One big difference between an E1 and a T1 is that an E1 bundles 32 time slots instead of 24. This difference results in a bandwidth of 2.048 Mb/s for an E1. With an E1 circuit, one time slot is used for framing and one is used for signaling, leaving 30 time slots available for user data.

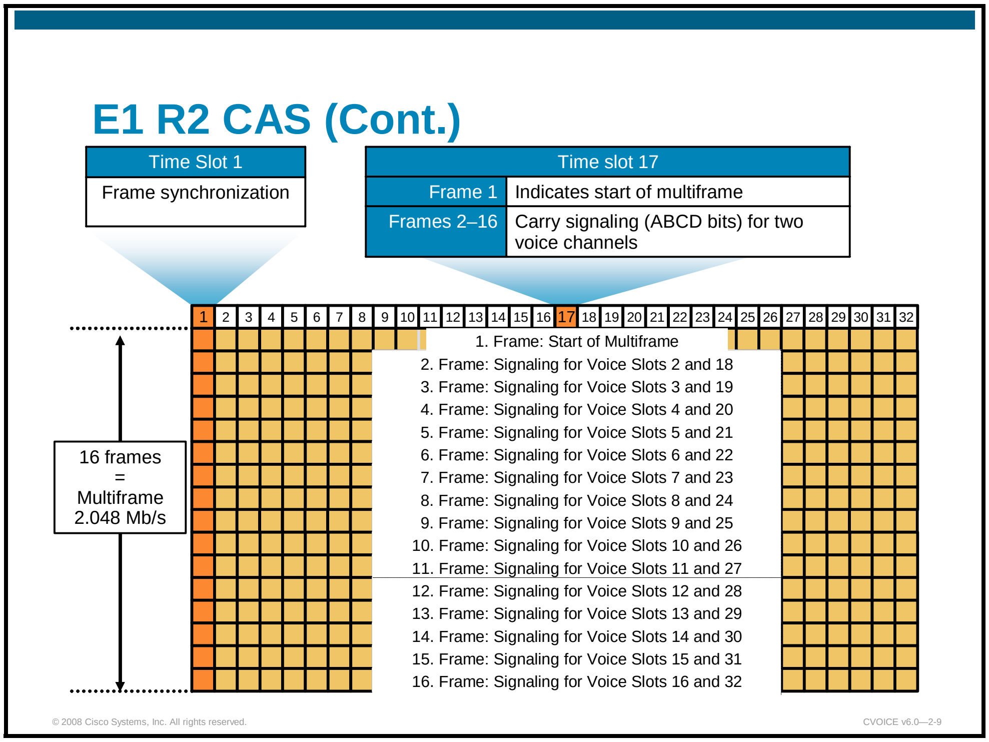
E1 R2 CAS Signaling

E1 digital circuits can be deployed using R2 signaling. These trunks are called E1 R2 trunks. To understand how E1 R2 signaling works, you need to understand the E1 multiframe format, which is used with E1 R2.

A multiframe consists of 16 consecutive 256-bit frames. Each frame carries 32 time slots. The first time slot is used exclusively for frame synchronization. Time slots 2 to 16 and 18 to 32 carry the actual voice traffic, and time slot 17 is used for R2 signaling.

The first frame in an E1 multiframe includes the multiframe format information in time slot 17. Frames 2 to 16 include the signaling information, each frame controlling two voice time slots.

Using this signaling method, E1R2 supports inbound and outbound DNIS and ANI.



E1 R2 CAS (Cont.)

Time Slot 1
Frame synchronization

Time slot 17	
Frame 1	Indicates start of multiframe
Frames 2–16	Carry signaling (ABCD bits) for two voice channels

1. Frame: Start of Multiframe
2. Frame: Signaling for Voice Slots 2 and 18
3. Frame: Signaling for Voice Slots 3 and 19
4. Frame: Signaling for Voice Slots 4 and 20
5. Frame: Signaling for Voice Slots 5 and 21
6. Frame: Signaling for Voice Slots 6 and 22
7. Frame: Signaling for Voice Slots 7 and 23
8. Frame: Signaling for Voice Slots 8 and 24
9. Frame: Signaling for Voice Slots 9 and 25
10. Frame: Signaling for Voice Slots 10 and 26
11. Frame: Signaling for Voice Slots 11 and 27
12. Frame: Signaling for Voice Slots 12 and 28
13. Frame: Signaling for Voice Slots 13 and 29
14. Frame: Signaling for Voice Slots 14 and 30
15. Frame: Signaling for Voice Slots 15 and 31
16. Frame: Signaling for Voice Slots 16 and 32

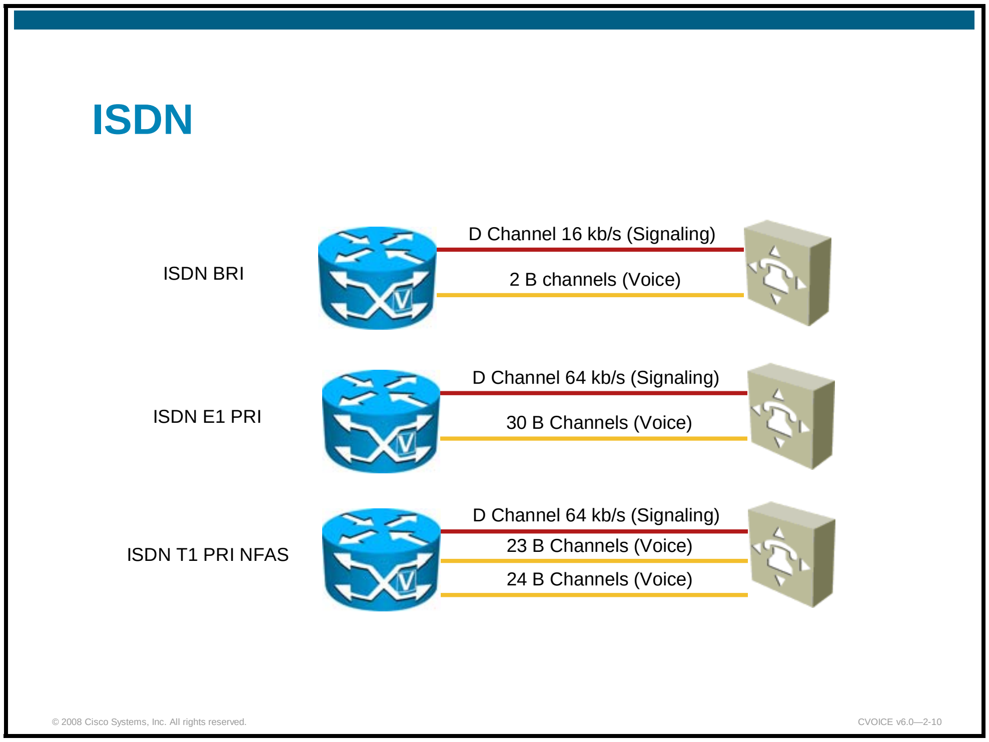
CVOICE v6.0—2-9

This figure shows the signaling concept that is used by E1 R2. Time slot 17 is used for signaling, and each of its frames carries information for two voice time slots. This results in the following frame allocation for signaling:

- **1. Frame, time slot 17:** Declares the multiframe
- **2. Frame, time slot 17:** Signaling for time slots 2 and 18
- **3. Frame, time slot 17:** Signaling for time slots 3 and 19
- **4. Frame, time slot 17:** Signaling for time slots 4 and 20
- **5. Frame, time slot 17:** Signaling for time slots 5 and 21
- **6. Frame, time slot 17:** Signaling for time slots 6 and 22
- **7. Frame, time slot 17:** Signaling for time slots 7 and 23
- **8. Frame, time slot 17:** Signaling for time slots 8 and 24
- **9. Frame, time slot 17:** Signaling for time slots 9 and 25
- **10. Frame, time slot 17:** Signaling for time slots 10 and 26
- **11. Frame, time slot 17:** Signaling for time slots 11 and 27
- **12. Frame, time slot 17:** Signaling for time slots 12 and 28
- **13. Frame, time slot 17:** Signaling for time slots 13 and 29
- **14. Frame, time slot 17:** Signaling for time slots 14 and 30
- **15. Frame, time slot 17:** Signaling for time slots 15 and 31
- **16. Frame, time slot 17:** Signaling for time slots 16 and 32

ISDN Overview

This topic describes ISDN.



ISDN

ISDN BRI

D Channel 16 kb/s (Signaling)

2 B channels (Voice)

ISDN E1 PRI

D Channel 64 kb/s (Signaling)

30 B Channels (Voice)

ISDN T1 PRI NFAS

D Channel 64 kb/s (Signaling)

23 B Channels (Voice)

24 B Channels (Voice)

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—2-10

Another protocol that is used for digital trunks is ISDN. ISDN is a circuit-switched telephone network system that is designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher speeds than is available with the PSTN system.

ISDN comprises digital telephony and data-transport services offered by regional telephone carriers. ISDN involves the digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires. The emergence of ISDN represents an effort to standardize subscriber services, user and network interfaces, and network and internetwork capabilities.

ISDN Services

In contrast to the CAS and R2 signaling, which provide only DNIS, ISDN offers additional supplementary services such as call waiting and Do Not Disturb (DND). ISDN applications include high-speed image applications (such as Group 4 [G4] fax), additional telephone lines in homes to serve the telecommuting industry, high-speed file transfer, and video conferencing. Voice service is also an application for ISDN.

ISDN Media Types

Cisco routing devices support ISDN BRI and ISDN PRI. Both media types use B channels and D channels. The B channels carry user data. The D channel, in its role as signal carrier for the B channels, directs the CO switch to send incoming calls to particular time slots on the Cisco access server or router. It also identifies the call as a circuit-switched digital call or an analog modem call. Circuit-switched digital calls are relayed directly to the ISDN processor in the router; analog modem calls are decoded and then sent to the onboard modems.

- **ISDN BRI:** Referred to as “2 B + D”:
  - — Two 64-kb/s B channels that carry voice or data for a maximum transmission speed of 128 kb/s
  - — One 16-kb/s D channel that carries signaling traffic, that is, instructions about how to handle each of the B channels, although it can support user data transmission under certain circumstances

  The D channel signaling protocol comprises Layers 1 through 3 of the Open Systems Interconnection (OSI) reference model. BRI also provides for framing control and other overhead, bringing its total bit rate to 192 kb/s.

  The BRI physical layer specification is ITU-T Recommendation I.430. BRI is very common in Europe and is also available in North America. BRI allows up to two simultaneous calls.

- **ISDN PRI:** Referred to as “23 B + D” or “30 B + D”:
  - — 23 B channels (in North America and Japan) or 30 B channels (in the rest of the world) that carry voice or data yielding a total bit rate of 1.544 Mb/s and 2.048 Mb/s respectively
  - — One 64-kb/s D channel that carries signaling traffic

  The PRI physical layer specification is ITU-T Recommendation I.431.

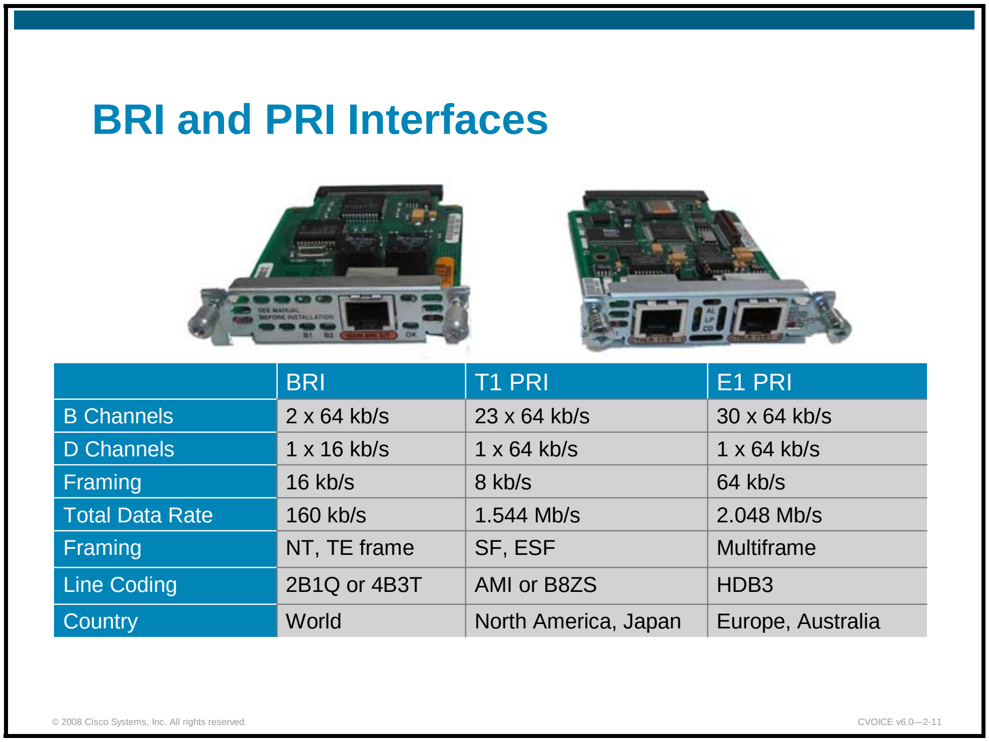
Note PRI is economically preferable to BRI because there is usually already an interface card supporting PRI in place on modern PBXs.

Following are three worldwide standards for PRI:

- — **T1 PRI:** Use this interface to designate North American ISDN PRI with 23 B channels and 1 CCS channel.
- — **E1 PRI:** Use this interface to designate European ISDN PRI with 30 B channels, 1 CCS channel, and 1 framing channel.
- — **ISDN PRI Non-Facility Associated Signaling (NFAS):** ISDN NFAS enables a single D channel to control multiple ISDN PRIs on a chassis. This D channel functions as the primary channel, with the option of having another D channel in the group as a backup. After you have configured the channelized controllers for ISDN NFAS, you need to configure only the NFAS primary D channel. Its configuration is distributed to all the members of the associated NFAS group. The benefit of PRI NFAS is that it frees the B channel by using a single D channel to control multiple PRI interfaces. One B channel on each interface is free to carry other traffic.
- — **Fractional PRI:** The term fractional PRI has different meanings in different parts of the world. One meaning indicates multiple PRI groups (B channels and an associated D channel) on the same T1/E1 interface. Because the High-Density Voice Network Module (NM-HDV) supports only a single D channel per T1/E1, the PRI feature does not support this definition of fractional PRI. However, the other meaning of the term indicates the ability to define a single D channel for each interface with less than 23 or 31 B channels associated with it. This definition of fractional PRI is supported.

BRI and PRI Interfaces

This subtopic describes BRI and PRI interfaces and their capabilities.



BRI and PRI Interfaces

	BRI	T1 PRI	E1 PRI
B Channels	2 x 64 kb/s	23 x 64 kb/s	30 x 64 kb/s
D Channels	1 x 16 kb/s	1 x 64 kb/s	1 x 64 kb/s
Framing	16 kb/s	8 kb/s	64 kb/s
Total Data Rate	160 kb/s	1.544 Mb/s	2.048 Mb/s
Framing	NT, TE frame	SF, ESF	Multiframe
Line Coding	2B1Q or 4B3T	AMI or B8ZS	HDB3
Country	World	North America, Japan	Europe, Australia

The figure illustrates the different capabilities of BRI and PRI interfaces.

Using ISDN for voice traffic has these benefits:

- ISDN is perfect for G.711 pulse code modulation (PCM) because each B channel is a full 64 kb/s with no robbed bits.
- ISDN has a built-in call control protocol known as ITU-T Recommendation Q.931.
- ISDN can convey standards-based voice features, such as speed dialing, automated operator services, call waiting, call forwarding, and geographic analysis of customer databases.
- ISDN supports standards-based enhanced dial up capabilities, such as G4 fax and audio channels.

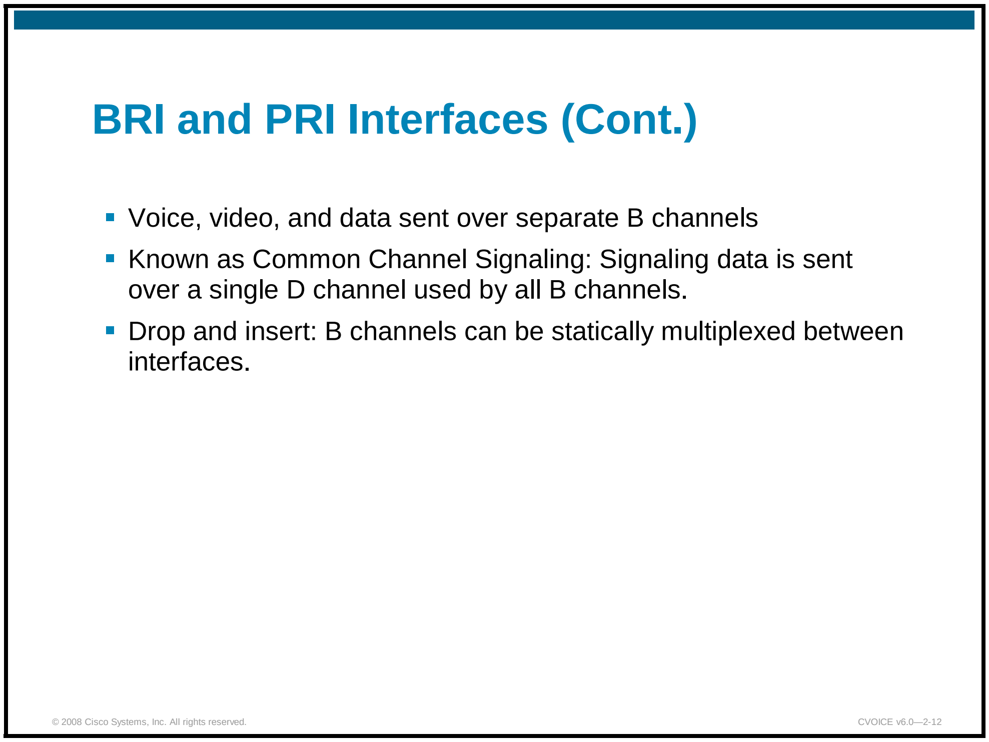
Line Coding

Digital T1/E1 interfaces require that line encoding be configured to match that of the PBX or CO that is being connected to the voice port. Line encoding defines the type of framing that is used on the line.

BRI line encoding methods include Two-Binary, One-Quaternary (2B1Q) and Four-Binary, Three-Ternary (4B3T). 2B1Q is a physical layer encoding used for Integrated Services Digital Network (ISDN) basic rate interface. 2B1Q uses four signal levels, which are -450 mV, -150 mV, 150 mV and 450 mV, each (1Q) equivalent to two bits (2B). 4B3T represents four binary bits using three pulses.

T1 PRI line encoding methods include alternate mark inversion (AMI) and binary 8-zero substitution (B8ZS). AMI is used on older T1 circuits and references signal transitions with a binary 1, or “mark.” B8ZS, a more reliable method, is more popular and is also recommended for PRI configurations. B8ZS encodes a sequence of eight zeros in a unique binary sequence to detect line-coding violations.

Supported E1 line encoding methods are AMI and high-density bipolar 3 (HDB3), which is a form of zero-suppression line coding.



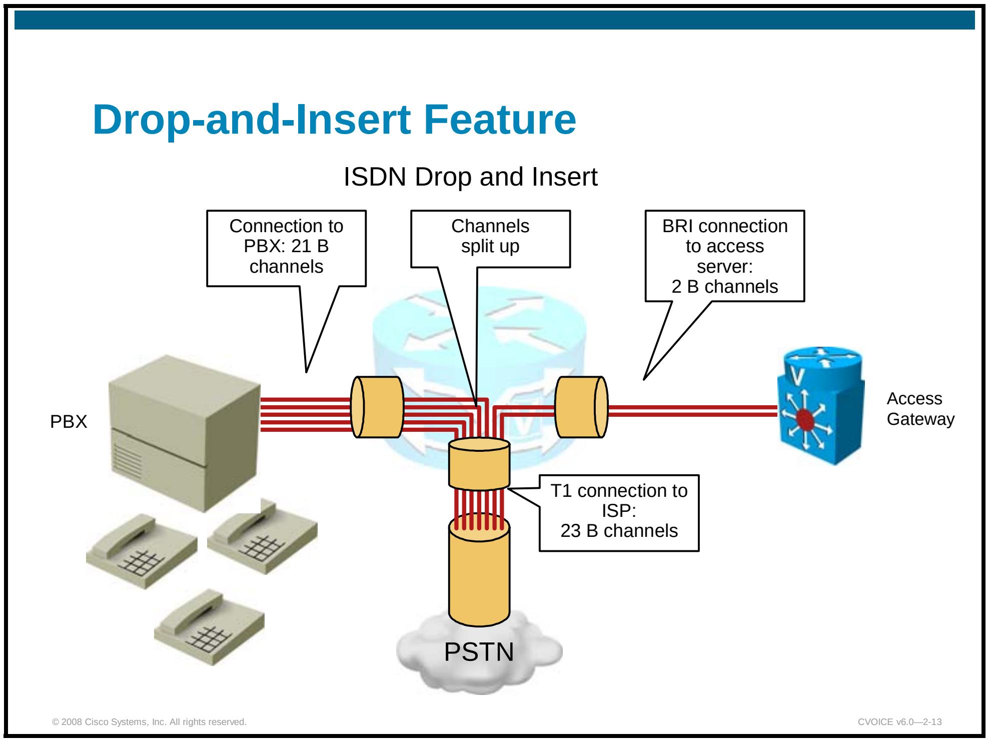
BRI and PRI Interfaces (Cont.)

- Voice, video, and data sent over separate B channels
- Known as Common Channel Signaling: Signaling data is sent over a single D channel used by all B channels.
- Drop and insert: B channels can be statically multiplexed between interfaces.

CVOICE v6.0—2-12

With ISDN, user data is separated from signaling data. User data, such as the payload from a digitized phone call, goes to a 64-kb/s B channel, and signaling data, such as a call setup message, goes to a D channel. A single D channel supports multiple B channels, which is why ISDN service is known as common channel signaling.

The drop-and-insert capability allows for dynamic multiplexing of the B channels between different interfaces. This feature is available only if all interfaces use a common clock source, as is the case with integrated services routers (ISRs).



Drop-and-Insert Feature

ISDN Drop and Insert

Connection to PBX: 21 B channels

Channels split up

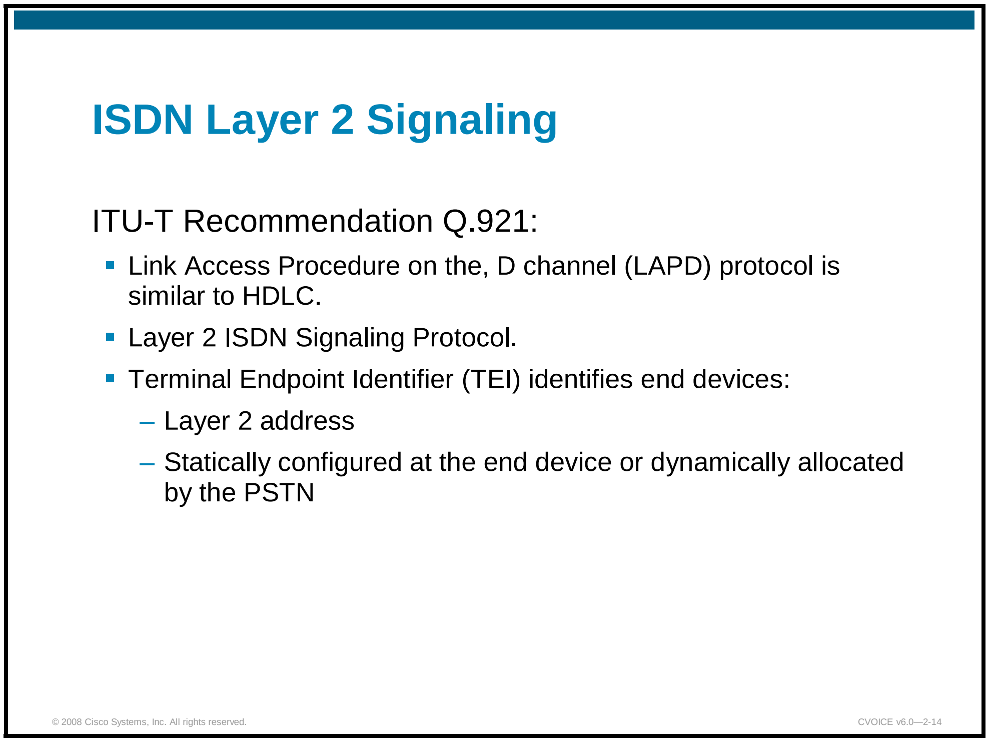
BRI connection to access server: 2 B channels

T1 connection to ISP: 23 B channels

This figure shows an example of the drop-and-insert feature. The channels of an ISDN PRI connection from the Internet service provider (ISP) are split up. Twenty-one channels are routed to another PRI interface of the router that is connected to a PBX, and two channels are routed to a BRI interface that is connected to an access server.

ISDN Signaling

This topic describes ISDN signaling.



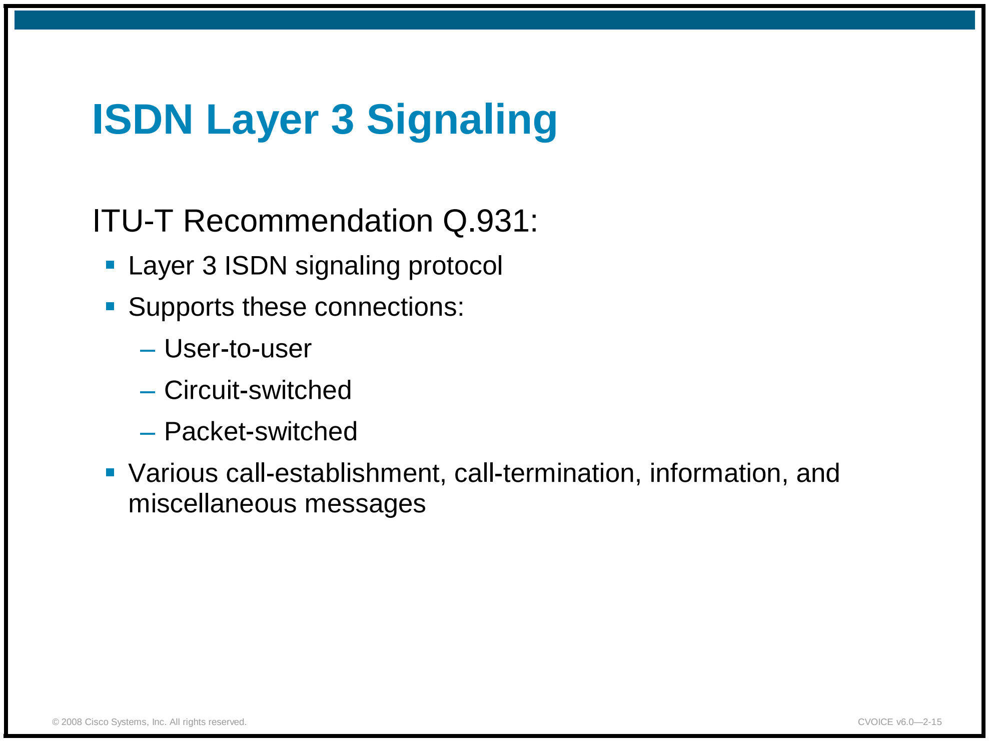
ISDN Layer 2 Signaling

ITU-T Recommendation Q.921:

- Link Access Procedure on the, D channel (LAPD) protocol is similar to HDLC.
- Layer 2 ISDN Signaling Protocol.
- Terminal Endpoint Identifier (TEI) identifies end devices:
  - Layer 2 address
  - Statically configured at the end device or dynamically allocated by the PSTN

CVOICE v6.0—2-14

Layer 2 of the ISDN signaling protocol is Link Access Procedure on the D channel (LAPD). LAPD is similar to High-Level Data Link Control (HDLC) and Link Access Procedure, Balanced (LAPB). As the expansion of the LAPD acronym indicates, this layer is used across the D channel to ensure that control and signaling information flows and is received properly. The LAPD frame format is very similar to that of HDLC. Like HDLC, LAPD uses supervisory information and unnumbered frames. The LAPD protocol is formally specified in ITU-T Recommendation Q.920 and ITU-T Recommendation Q.921. The Terminal Endpoint Identifier (TEI) field identifies either a single terminal or multiple terminals. A TEI of all 1s indicates a broadcast.



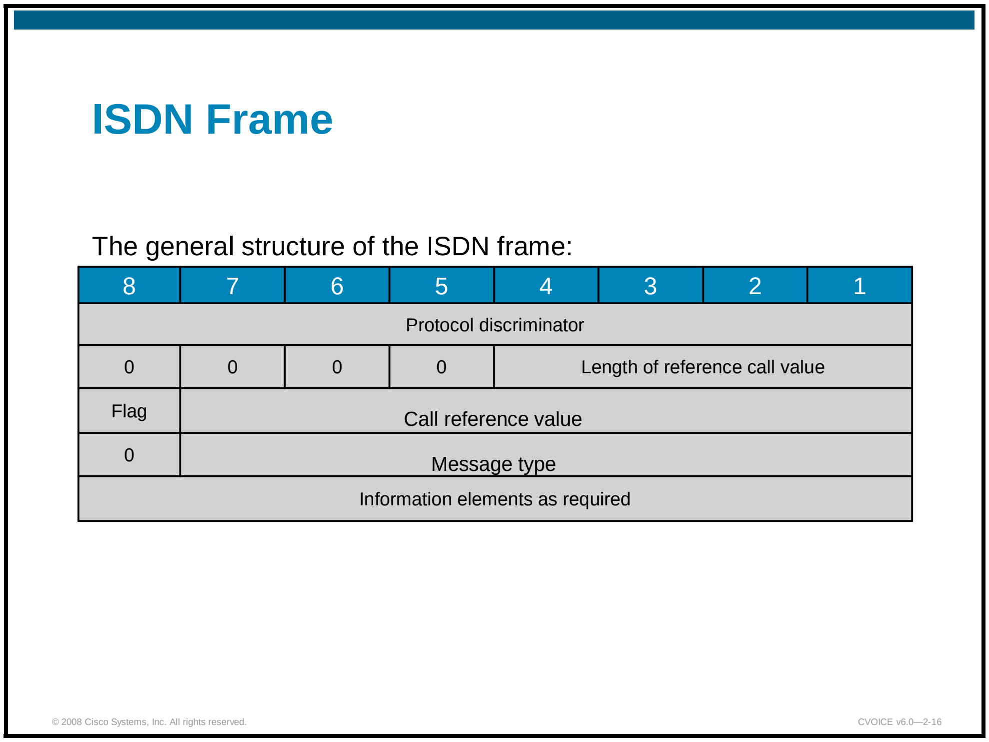
ISDN Layer 3 Signaling

ITU-T Recommendation Q.931:

- Layer 3 ISDN signaling protocol
- Supports these connections:
  - User-to-user
  - Circuit-switched
  - Packet-switched
- Various call-establishment, call-termination, information, and miscellaneous messages

CVOICE v6.0—2-15

Two Layer 3 specifications are used for ISDN signaling: ITU-T Recommendation I.450 (also known as ITU-T Recommendation Q.930) and ITU-T Recommendation I.451 (also known as ITU-T Recommendation Q.931). Together, these protocols support user-to-user, circuit-switched (the B channels), and packet-switched (the D channel) connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol. X.25 is an ITU-T standard protocol suite used for connections to packet-switched, wide-area networks using leased lines, the phone system, or ISDN system as the networking hardware.



ISDN Frame

The general structure of the ISDN frame:

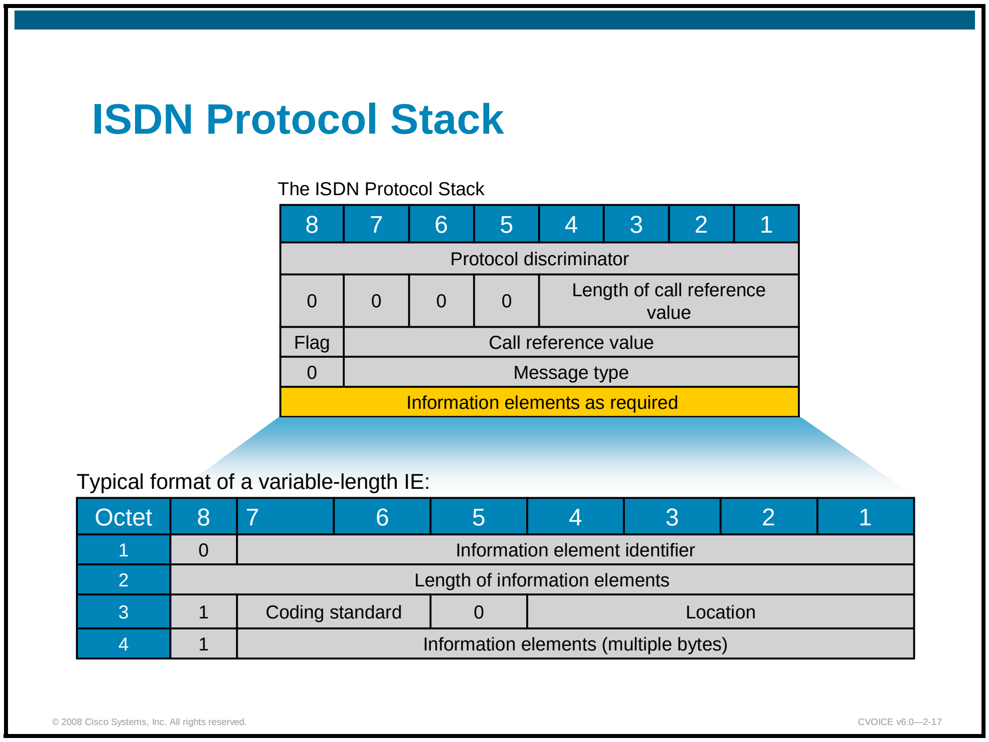
8	7	6	5	4	3	2	1
Protocol discriminator							
0	0	0	0	Length of reference call value			
Flag	Call reference value						
0	Message type						
Information elements as required							

Because ISDN message types may influence the function of a BRI or PRI trunk configuration, you should examine the messages that are part of the Q.931 packet structure and see how ISDN carries out the signaling function.

ISDN signaling takes place in the D channel and uses a message-oriented protocol that supports call control signaling and packet data. In its role as signal carrier for the B channels, the D channel directs the CO switch to send incoming calls to particular time slots on the Cisco access server or router.

Following are the components of the ISDN frame that are used to transmit these instructions:

- **Protocol discriminator:** This is the protocol that is used to encode the remainder of the layer.
- **Length of call reference value:** This defines the length of the next field. The call reference may be one or two octets long depending on the size of the value being encoded.
- **Flag:** This is set to zero (0) for messages sent by the party that allocated the call reference value; otherwise, it is set to one (1).
- **Call reference value:** This is an arbitrary value that is allocated for the duration of the specific session. This value identifies the call between the device maintaining the call and the ISDN switch.
- **Message type:** This identifies the message type (for example, SETUP) that determines what additional information is required and allowed. The message type may be one or more octets. When there is more than one octet, the first octet is coded as eight 0s.
- **ISDN information element:** Most D channel messages include additional information needed for call processing, such as the calling party number, called party number, and channel ID (CID). The additional information in a message is passed in information elements.



ISDN Protocol Stack

The ISDN Protocol Stack

8	7	6	5	4	3	2	1
Protocol discriminator							
0	0	0	0	Length of call reference value			
Flag	Call reference value						
0	Message type						
Information elements as required							

Typical format of a variable-length IE:

Octet	8	7	6	5	4	3	2	1
1	0	Information element identifier						
2	Length of information elements							
3	1	Coding standard		0	Location			
4	1	Information elements (multiple bytes)						

CVOICE v6.0—2-17

ISDN sends instructions in Layer 3 messages that are put into Layer 2 frames and are finally time-multiplexed onto a medium with either a BRI or a PRI Layer 1 line coding specification.

A depiction of D-channel messages is shown in the figure. These messages allow complete control over call establishment and clearing, network maintenance, and the passing of other call-related information between switches.

The additional information that is required by an ISDN message is passed in information elements and varies depending on the message type, the action being performed, and the connected equipment. Mandatory and optional information elements for D-channel messages are defined in ITU-T Recommendation Q.931.

An information element can be a single byte or several bytes, and by reading the message, the switch can determine this information. For example, in octet 1 of the information element, if bit 8, or the extension bit, is 0, the information element is of a variable length. If the bit is 1, the information element is a single byte.

The information contained in octet 3 is the coding standard and the location. The “Coding Standard” and “Location” tables provide the possible content of these fields.

Coding Standard

Bit Sequence	Meaning
00	ITU standardized coding
11	Standard specific to the location field

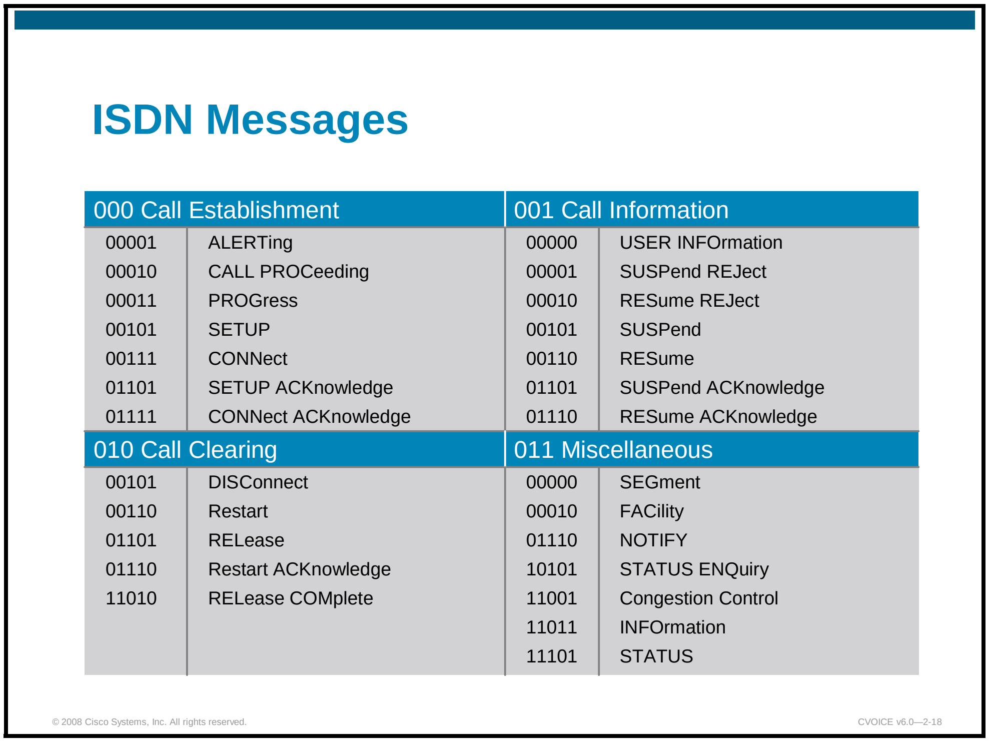
Location

Bit Sequence	Meaning
0000	User
0001	Private network serving the local user
0010	Public network serving the local user
0011	Transit network
0100	Public network serving the remote user
0101	Remote private network
0111	International network
1010	Network beyond the interworking point

A called number is passed to the PSTN by an information element. The information element contains bytes describing the numbering plan and the type of number. Typically, the numbering type is not changed; however, there may be times when a network administrator elects to have a specific gateway handle all international calls. If this connection to the PSTN is an ISDN PRI, the information element must tell the PSTN that the called number is in international format.

ISDN Messages

This subtopic covers ISDN messages.



ISDN Messages

000 Call Establishment		001 Call Information	
00001	ALERTing	00000	USER INFOrmation
00010	CALL PROCeeding	00001	SUSPend REJect
00011	PROGress	00010	RESume REJect
00101	SETUP	00101	SUSPend
00111	CONNect	00110	RESume
01101	SETUP ACKnowledge	01101	SUSPend ACKnowledge
01111	CONNect ACKnowledge	01110	RESume ACKnowledge
010 Call Clearing		**011 Miscellaneous**	
00101	DISConnect	00000	SEGment
00110	Restart	00010	FACility
01101	RELease	01110	NOTIFY
01110	Restart ACKnowledge	10101	STATUS ENQuiry
11010	RELease COMplete	11001	Congestion Control
		11011	INFOrmation
		11101	STATUS

CVOICE v6.0—2-18

ISDN signaling is carried out by messages that are sent between endpoints on the D channel. The message type is a single byte (octet) that indicates what type of message is being sent or received. There are four general categories of messages that might be present: call establishment, call information, call clearing, and miscellaneous. Generally, the most useful messages to understand are the call establishment and call clearing messages. The most common messages are listed in the table.

The "Most Common Message Types and Associated Information Elements" table below provides a list of message types and the information elements that can be associated with each message.

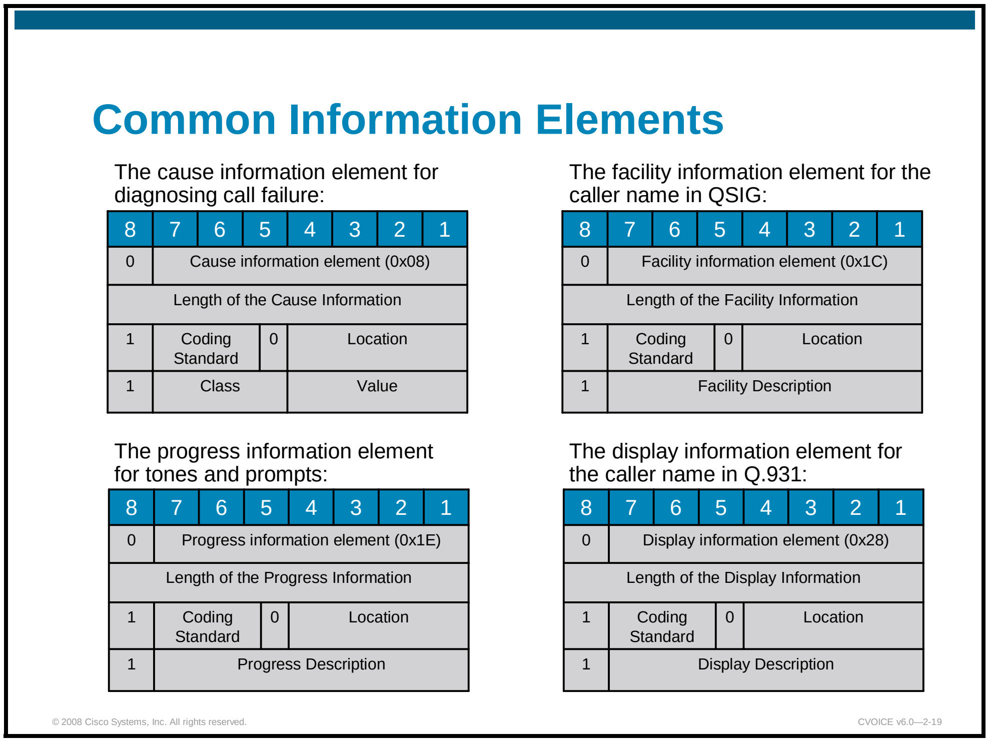
Most Common Message Types and Associated Information Elements

Message Type	Information Elements Associated with Message
ALERTing	Bearer capability, CID, progress indicator, display, signal, higher layer compatibility
CALL PROCeeding	Bearer capability, CID, progress indicator, display, higher layer compatibility
SETUP	Sending complete, repeat indicator, bearer capability, CID, progress indicator, network specific facilities, display, keypad facility, signal, calling party number, calling party sub address, called party number, called party sub address, transit network selection, repeat indicator, lower layer compatibility, higher layer compatibility
CONNect	Bearer capability, CID, progress indicator, display, date/time, signal, lower layer compatibility, higher layer compatibility

Message Type	Information Elements Associated with Message
SETUP ACKnowledge	CID, progress indicator, display, signal
CONNect ACKnowledge	Display, signal
DISConnect	Cause, progress indicator, display, signal
RELease	Cause, display, signal
RELease COMplete	Cause, display, signal
STATUS ENQuiry	Display
STATUS	Cause, call state, display

ISDN Information Element

This subtopic covers ISDN information elements.



Common Information Elements

The cause information element for diagnosing call failure:

8	7	6	5	4	3	2	1
0	Cause information element (0x08)						
Length of the Cause Information							
1	Coding Standard		0	Location			
1	Class			Value			

The facility information element for the caller name in QSIG:

8	7	6	5	4	3	2	1
0	Facility information element (0x1C)						
Length of the Facility Information							
1	Coding Standard		0	Location			
1	Facility Description						

The progress information element for tones and prompts:

8	7	6	5	4	3	2	1
0	Progress information element (0x1E)						
Length of the Progress Information							
1	Coding Standard		0	Location			
1	Progress Description						

The display information element for the caller name in Q.931:

8	7	6	5	4	3	2	1
0	Display information element (0x28)						
Length of the Display Information							
1	Coding Standard		0	Location			
1	Display Description						

CVOICE v6.0—2-19

Each type of message has mandatory and optional information elements associated with it. The information element is identified with a single byte (octet). While there are a few single octet (byte) information elements, most have multiple octets associated with them.

A study of all available information elements is beyond the scope of this course. Commonly used information elements are listed in the "ISDN Progress Description Field Values" table. For further details, there are many public references that are available on the Internet. For this lesson, the cause, facility, progress, and display information elements are reviewed. They represent the information most in demand in telephony systems and, therefore, most important in the communications between the voice gateway and PBX or PSTN.

Cause Information Element

The cause information element provides one or more octets that may help in diagnosing network or customer premises equipment (CPE) problems. When a call is terminated, a cause ID indicates the reason for the termination. Both sides can generate a cause ID, and cause IDs are created for every call. When there is an ISDN problem in the network, the cause value, shown in octet 4 in the figure, represents useful debug information in the ISDN protocol log. The telephone company equipment translates these values to associated phrases. Cause messages are classified as normal events, resource or service availability, message validity, protocol error, or interworking. The most common phrases are listed in the "Common Information Elements" table.

Facility Information Element

Supplemental services are invoked by sending facility information elements in a facility message to an ISDN switching device such as a PBX.

Supplemental services are widely used by PBXs and in the PSTN. IP telephony systems that are connected to these types of switches must be able to send and receive these messages. The supplemental service and associated parameters that are invoked are PBX-specific and should be provided by the PBX manufacturer.

Progress Information Element

Progress tones such as ringback and busy tones, and announcements such as “The number you have dialed is no longer in service,” are required to successfully signal voice calls. Progress tones can be generated by the originating, terminating, or intermediate devices.

The indication of in-band tones and announcements is controlled by the progress information element in ISDN and H.323 networks. The progress information element signals those interworking situations where in-band tones and announcements must be used.

The indication that tones and announcements are available is signaled by an ALERTING, CALL PROCEEDING, PROGRESS, CONNECT, SETUP ACKNOWLEDGE, or DISCONNECT message containing a progress indicator (PI) of PI = 1 or 8, which would be sent in the progress description field in octet 4.

A SETUP message of PI = 3 means that the switch is indicting to the originating gateway that in-band messages are expected.

ISDN Progress Description Field Values

Hex Value	Decimal	Binary	Description
0x01	1	000 0001	Call is not end-to-end ISDN.
0x02	2	000 0010	Destination address is non-ISDN.
0x03	3	000 0011	Origination address is non-ISDN.
0x04	4	000 0100	Call has returned to the ISDN.
0x08	8	000 1000	In-band information or the appropriate pattern is now available.
0x0A	10	000 1010	There is a delay in response at the destination interface.

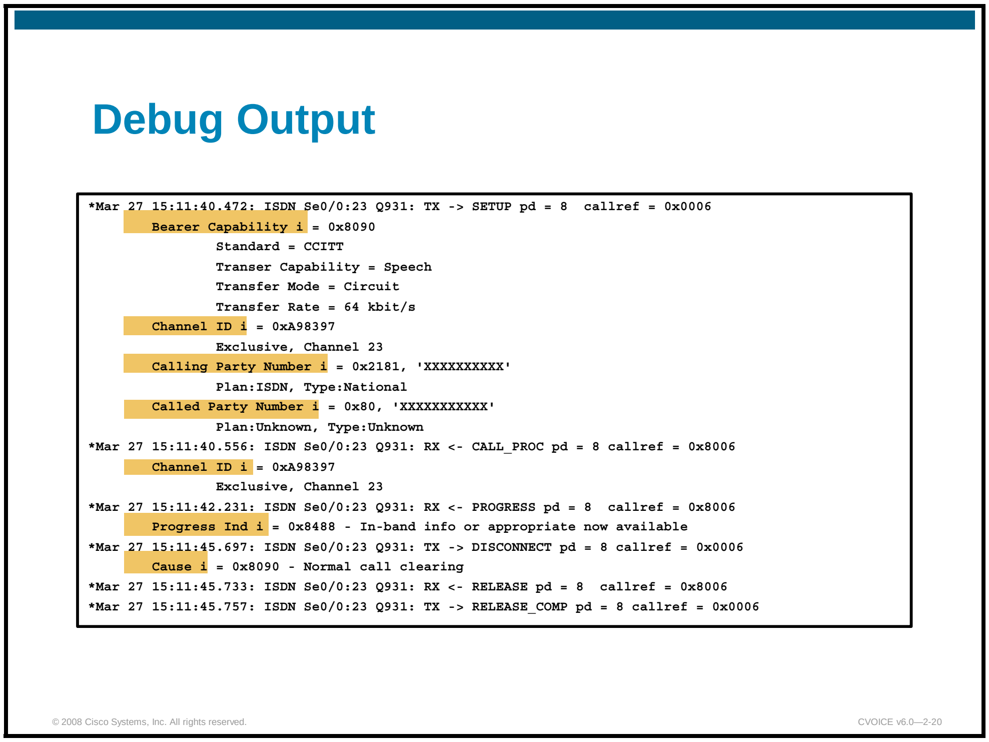
Display Information Element

The display information element sends text to do such things as provide output for an LCD display. This information element is commonly used to pass caller name information over a PRI, although there are PBXs and telecommunications service providers with National ISDN 3 (NI3) switches that only pass calling name information with the facility information element in Q Signaling (QSIG). The display and facility information elements are used by Cisco Unified Communications Manager to support caller name and number identification presentation. These services are based on the device control protocols that handle the call. Not all device protocols provide caller number and name information in the protocol messages.

Common Information Elements

<table>
<tr><th>Value</th><th>Name</th><th colspan="2">Description</th></tr>
<tr><td>0x04</td><td>Bearer</td><td colspan="2">Specifies packet or circuit mode, data rate, and type of information content (voice).</td></tr>
<tr><td rowspan="12">0x08</td><td rowspan="12">Cause</td><td colspan="2">Provides the reason a call was rejected or disconnected. Here is a sample of possible causes:</td></tr>
<tr><td>0x01</td><td>Unassigned number</td></tr>
<tr><td>0x03</td><td>No route to destination</td></tr>
<tr><td>0x06</td><td>Channel unacceptable</td></tr>
<tr><td>0x10</td><td>Normal call clearing</td></tr>
<tr><td>0x11</td><td>User busy</td></tr>
<tr><td>0x12</td><td>User not responding</td></tr>
<tr><td>0x13</td><td>User alerting; no answer</td></tr>
<tr><td>0x1B</td><td>Destination out of order</td></tr>
<tr><td>0x1C</td><td>Invalid number format</td></tr>
<tr><td>0x22</td><td>No circuit or channel available</td></tr>
<tr><td>0x2A</td><td>Switching equipment congestion</td></tr>
<tr><td>0x14</td><td>Call state</td><td colspan="2">Is the current status of a call in terms of the standard Q.931 state machine.</td></tr>
<tr><td>0x18</td><td>CID</td><td colspan="2">Defines the B channel that is being used.</td></tr>
<tr><td>0x1C</td><td>Facility</td><td colspan="2">Indicates the invocation and operation of supplemental services, identified by the corresponding operation value within the facility information element. Here are some examples of supplemental services:
■ Called or calling party identification
■ Subaddressing
■ Hold or retrieve
■ Call transfer
■ Message waiting</td></tr>
<tr><td rowspan="7">0x1E</td><td rowspan="7">Progress indication</td><td colspan="2">Provides information about the call in progress. Here are some examples of progress indication:</td></tr>
<tr><td>0x01</td><td>Call is not end-to-end ISDN.</td></tr>
<tr><td>0x02</td><td>Destination address is non-ISDN.</td></tr>
<tr><td>0x03</td><td>Origination address is non-ISDN.</td></tr>
<tr><td>0x04</td><td>Call has returned to the ISDN.</td></tr>
<tr><td>0x08</td><td>In-band information or the appropriate pattern is now available.</td></tr>
<tr><td>0x0A</td><td>Delay in response at the destination interface.</td></tr>
<tr><td>0x28</td><td>Display</td><td colspan="2">Provides human-readable text that can be specified with almost any message (for example, to provide text for an LCD display).</td></tr>
<tr><td>0x2C</td><td>Keypad</td><td colspan="2">Dialed digits.</td></tr>
</table>

Value	Name	Description		
0x34	Signal	Provides call status tones according to this chart:		
		0x00	Dial tone	350 Hz + 440 Hz; continuous
		0x01	Ringing	440 Hz + 480 Hz; 2 sec on and 4 sec off
		0x02	Intercept	Alternating 440 Hz and 620 Hz; 250 ms
		0x03	Network congestion (fast busy)	480 Hz + 620 Hz; 250 ms on and 250 ms off
		0x04	Busy	480 Hz + 620 Hz; 500 ms on and 500 ms off
		0x05	Confirm	350 Hz + 440 Hz; repeated three times: 100 ms on and 100 ms off
		0x06	Answer	Not used
		0x07	Call waiting	440 Hz; 300 ms burst
		0x08	Off-hook warning	1400 Hz + 2060 Hz + 2450 Hz + 2600 Hz; 100 ms on and 100 ms off
		0x3F	Tones	Off
0x3A	SPID	Contains a service profile identifier (SPID).		
0x4C	Connected number	Is the remaining caller if a disconnect occurs during a conference.		
0x6C	Calling party number	Is the origin phone number.		
0x70	Called party number	Is the dialed phone number.		
0x7C	LLC	Defines the lower-layer compatibility.		
0x7D	HLC	Defines the higher layer compatibility.		
0x7E	User-user	Defines the user-user information.		



Debug Output

```
*Mar 27 15:11:40.472: ISDN Se0/0:23 Q931: TX -> SETUP pd = 8  callref = 0x0006
        Bearer Capability i = 0x8090
                Standard = CCITT
                Transer Capability = Speech
                Transfer Mode = Circuit
                Transfer Rate = 64 kbit/s
        Channel ID i = 0xA98397
                Exclusive, Channel 23
        Calling Party Number i = 0x2181, 'XXXXXXXXXX'
                Plan:ISDN, Type:National
        Called Party Number i = 0x80, 'XXXXXXXXXXX'
                Plan:Unknown, Type:Unknown
*Mar 27 15:11:40.556: ISDN Se0/0:23 Q931: RX <- CALL_PROC pd = 8 callref = 0x8006
        Channel ID i = 0xA98397
                Exclusive, Channel 23
*Mar 27 15:11:42.231: ISDN Se0/0:23 Q931: RX <- PROGRESS pd = 8  callref = 0x8006
        Progress Ind i = 0x8488 - In-band info or appropriate now available
*Mar 27 15:11:45.697: ISDN Se0/0:23 Q931: TX -> DISCONNECT pd = 8 callref = 0x0006
        Cause i = 0x8090 - Normal call clearing
*Mar 27 15:11:45.733: ISDN Se0/0:23 Q931: RX <- RELEASE pd = 8  callref = 0x8006
*Mar 27 15:11:45.757: ISDN Se0/0:23 Q931: TX -> RELEASE_COMP pd = 8 callref = 0x0006
```

Several sources are available on Cisco.com to help you read the output from a **debug isdn q931** command.

- The "ISDN Codes" chapter in the *Cisco IOS Debug Command Reference, Release 12.4T:* http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_chapter09186a00804ab4b9.html
- The **debug isdn q931** command in the *Debug Command Reference* at http://www.cisco.com/en/US/partner/products/ps6441/products_command_reference_chapter09186a00804ab699.html#wp1012971.

The "ISDN Bearer Capability Values" table, taken from the *Debug Command Reference* provides an example of how to read the hexadecimal values with the ISDN bearer capability values.

ISDN Bearer Capability Values

Field	Value Description
0x	Indication that the values that follow are in hexadecimal
88	ITU-T coding standard; unrestricted digital information
90	Circuit mode, 64 kb/s
21	Layer 1, V.110/X.30
8F	Synchronous, no in-band negotiation, 56 kb/s
0x8090A2	Voice call (mu-law)
0x9090A2	Voice call (mu-law), 3.1 kHz audio
0x8090A3	Voice call (a-law)
0x9090A3	Voice call (a-law), 3.1 kHz audio

Field 0x8890 is for 64 kb/s and 0x218F is for 56 kb/s. In the figure, the SETUP message in the example configuration indicates that **Bearer Capability i = 0x8090**. Therefore, you know that you have a 64-kb/s bearer stream.

The figure shows that i = 0x y1 y2 z1 z2 [a1 a2].

Following is a table of cause code fields.

ISDN Cause Code Fields

Field	Value: Description
0x	The values that follow are in hexadecimal.
y1	8: ITU-T standard coding.
y2	0: User 1: Private network serving local user 2: Public network serving local user 3: Transit network 4: Public network serving remote user 5: Private network serving remote user 7: International network A: Network beyond internetworking point
z1	Class (the more significant hexadecimal number) of cause value.
z2	Value (the less significant hexadecimal number) of cause value.
a1	(Optional) Diagnostic field that is always 8.
a2	(Optional) Diagnostic field that is one of the following values: 0: Unknown 1: Permanent 2: Transient

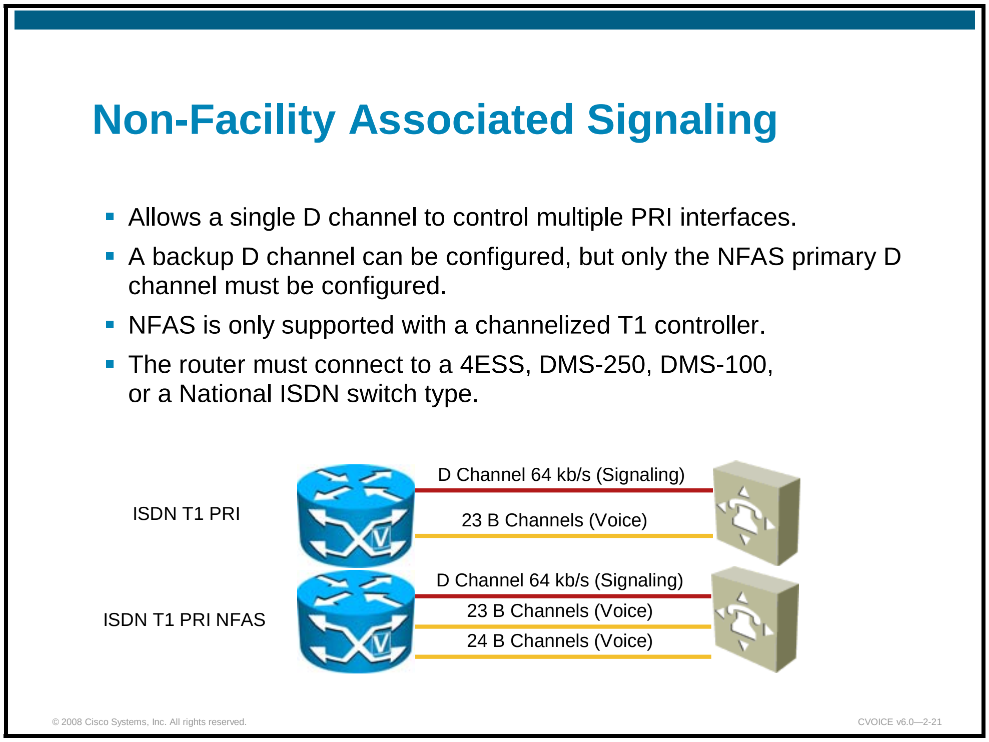
The following table lists some of the cause value fields of the cause information element.

ISDN Cause Values

Decimal	Hexadecimal	Cause	Explanation
30	1E	Response to STATUS ENQUIRY	The status message was generated in direct response to the prior receipt of a STATUS ENQUIRY message.
31	1F	Normal, unspecified	Reports the occurrence of a normal event when no standard cause applies. No action required.
34	22	No circuit or channel available	The connection cannot be established because no appropriate channel is available to take the call.

Non-Facility Associated Signaling

This subtopic describes NFAS.



Non-Facility Associated Signaling

- Allows a single D channel to control multiple PRI interfaces.
- A backup D channel can be configured, but only the NFAS primary D channel must be configured.
- NFAS is only supported with a channelized T1 controller.
- The router must connect to a 4ESS, DMS-250, DMS-100, or a National ISDN switch type.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-21

ISDN NFAS allows a single D channel to control multiple PRI interfaces. Use of a single D channel to control multiple PRI interfaces frees one B channel on each interface to carry other traffic. A backup D channel can be configured for use when the primary NFAS D channel fails. When a backup D channel is configured, any hard system failure causes a switchover to the backup D channel and currently connected calls remain connected.

NFAS is supported only with a channelized T1 controller and, as a result, must be ISDN PRI-capable. Once the channelized T1 controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all members of the associated NFAS group. Any configuration changes made to the primary D channel will be propagated to all NFAS group members. The primary D channel interface is the only interface shown after the configuration is written to memory.

The channelized T1 controllers on the router must also be configured for ISDN. The router must connect to either an AT&T 4ESS, Nortel DMS-100 or DMS-250, or National ISDN switch type.

The ISDN switch must be provisioned for NFAS. The primary and backup D channels should be configured on separate T1 controllers. The primary, backup, and B-channel members on the respective controllers should be the same configuration as that configured on the router and ISDN switch. The interface ID assigned to the controllers must match that of the ISDN switch.

You can disable a specified channel or an entire PRI interface, thereby taking it out of service or placing it into one of the other states that is passed in to the switch using the **isdn service** interface configuration command.

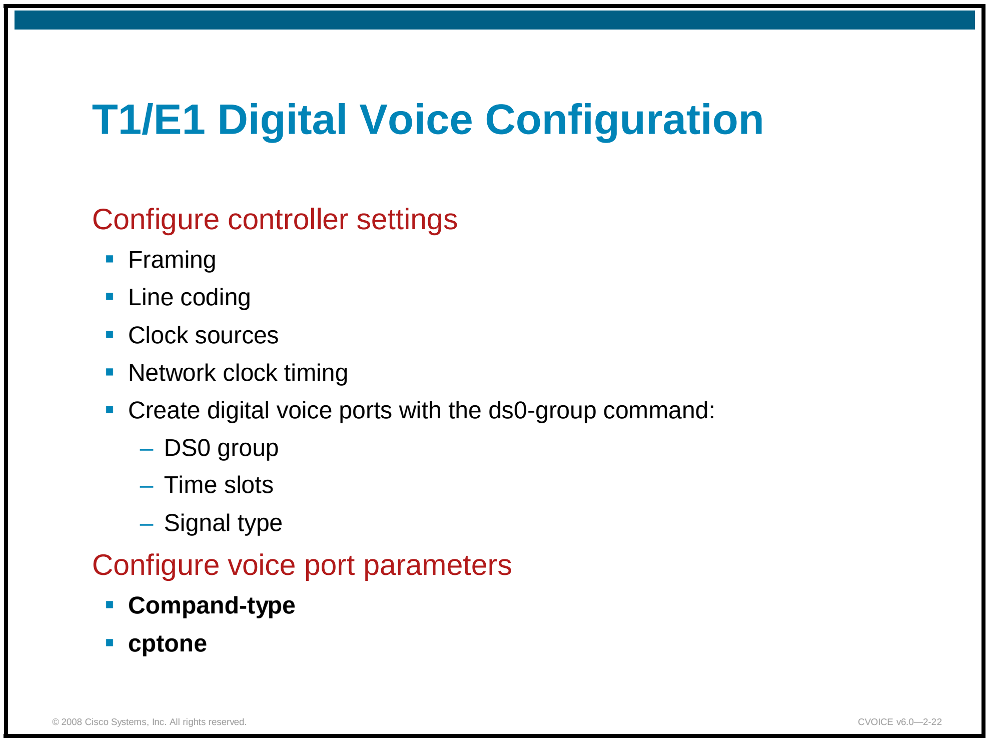
In the event that a controller belonging to an NFAS group is shut down, all active calls on the controller that is shut down will be cleared (regardless of whether the controller is set to primary, backup, or none), and one of the following events will occur:

- If the controller that is shut down is configured as the primary and no backup is configured, all active calls on the group are cleared.
- If the controller that is shut down is configured as the primary, and the active (in service) D channel is the primary and a backup is configured, then the active D channel changes to the backup controller.
- If the controller that is shut down is configured as the primary, and the active D channel is the backup, then the active D channel remains as backup controller.
- If the controller that is shut down is configured as the backup, and the active D channel is the backup, then the active D channel changes to the primary controller.

The expected behavior in NFAS when an ISDN D channel (serial interface) is shut down is that ISDN Layer 2 should go down but keep ISDN Layer 1 up, and that the entire interface will go down after the amount of seconds specified for timer T309.

Configuring T1 CAS Trunks

This topic describes how to configure T1 CAS trunks to the PSTN.



T1/E1 Digital Voice Configuration

Configure controller settings

- Framing
- Line coding
- Clock sources
- Network clock timing
- Create digital voice ports with the ds0-group command:
  - DSO group
  - Time slots
  - Signal type

Configure voice port parameters

- **Compand-type**
- **cptone**

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-22

Before configuring a T1 or E1 trunk you must gather the following information about the telephony network connection of the voice port:

- Framing formats
- Line coding
- Clock sources
- Network clock timing
- DS0 groups

These parameters are explained in more detail in the following subtopics.

Framing Formats

The framing format parameter describes the way that bits are robbed from specific frames to be used for signaling purposes. The controller must be configured to use the same framing format as the line from the PBX or CO that connects to the voice port that you are configuring.

Digital T1 lines use SF or ESF framing formats. SF provides two-state, continuous supervision signaling, in which bit values of 0 are used to represent on-hook states and bit values of 1 are used to represent off-hook states. ESF robs four bits instead of two, yet it has little impact on voice quality. ESF is required for 64-kb/s operation on DS0 and is recommended for PRI configurations.

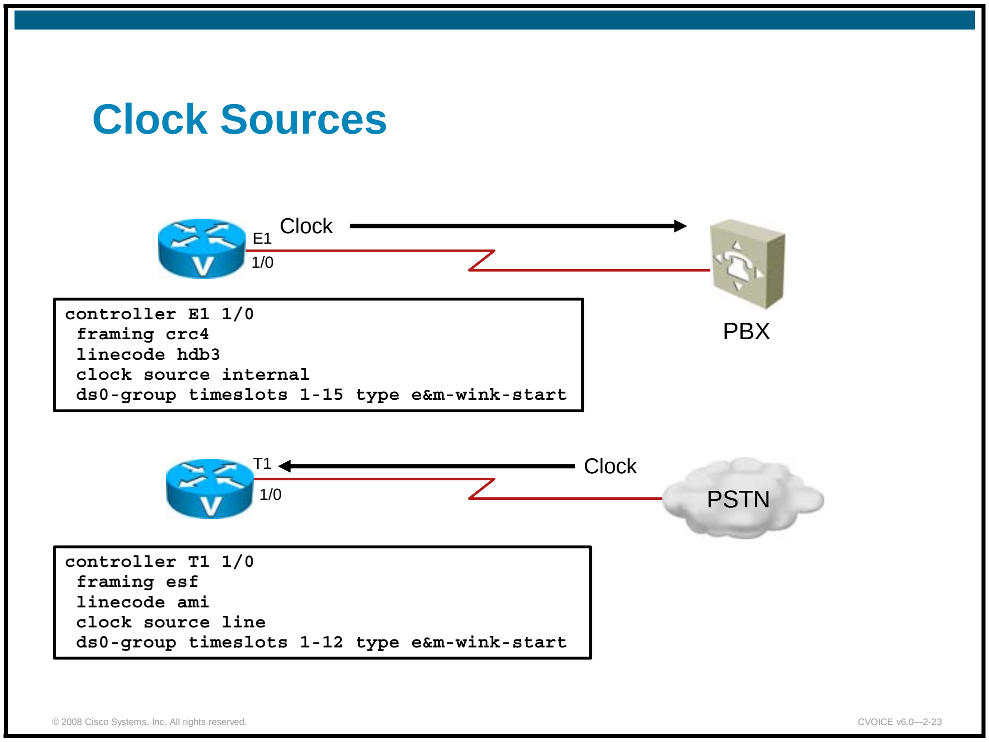
E1 lines can be configured for cyclic redundancy check 4 (CRC4) or no CRC, with an optional argument for E1 lines in Australia.

Line Coding

Digital T1/E1 interfaces require that line encoding be configured to match that of the PBX or CO that is being connected to the voice port. Line encoding defines the type of framing that is used on the line.

T1 line encoding methods include alternate mark inversion (AMI) and binary 8-zero substitution (B8ZS). AMI is used on older T1 circuits and references signal transitions with a binary 1, or “mark.” B8ZS, a more reliable method, is more popular and is also recommended for PRI configurations. B8ZS encodes a sequence of eight zeros in a unique binary sequence to detect line-coding violations.

Supported E1 line encoding methods are AMI and high-density bipolar 3 (HDB3), which is a form of zero-suppression line coding.



Clock Sources

```
controller E1 1/0
 framing crc4
 linecode hdb3
 clock source internal
 ds0-group timeslots 1-15 type e&m-wink-start
```

```
controller T1 1/0
 framing esf
 linecode ami
 clock source line
 ds0-group timeslots 1-12 type e&m-wink-start
```

Clock Sources

Digital T1/E1 interfaces use timers called “clocks” to ensure that voice packets are delivered and assembled properly. All interfaces handling the same packets must be configured to use the same source of timing so that packets are not lost or delivered late. The timing source that is configured can be external (from the line) or internal to the router digital interface.

If the timing source is internal, timing derives from the onboard phase lock loop (PLL) chip in the digital voice interface. If the timing source is line (external), then timing derives from the PBX or PSTN CO to which the voice port is connected. It is generally preferable to derive timing from the PSTN because its clocks are maintained at an extremely accurate level. External timing is the default setting for the clocks. When two or more controllers are configured, one should be designated as the primary clock source; it will drive the other controllers.

The figure depicts the following types of clocking:

- **Single voice port providing clocking:** In this scenario, the digital voice hardware is the clock source for the connected device, as shown in the figure above. The PLL generates the clock internally and drives the clocking on the line. Generally, this method is useful only for connections to a PBX, key system, or channel bank. A Cisco VoIP gateway rarely provides clocking *to* the CO because CO clocking is much more reliable.
- **Single voice port receiving internal clocking:** In this scenario, the digital voice hardware receives clocking from the connected device (CO telephony switch or PBX). The PLL clocking is driven by the clock reference on the receive (Rx) side of the digital line connection.

Network Clock Timing

Voice systems that pass digitized (or PCM) speech have always relied on the clocking signal being embedded in the received bit stream. This reliance allows connected devices to recover the clock signal from the bit stream, and then use this recovered clock signal to ensure that data on different channels keeps the same timing relationship with other channels.

If a common clock source is not used between devices, the binary values in the bit streams may be misinterpreted because the device samples the signal at the wrong moment. As an example, if the local timing of a receiving device is using a slightly shorter time period than the timing of the sending device, a string of eight continuous binary 1s may be interpreted as nine continuous 1s. If this data is then resent to devices that are further downstream that use varying timing references, the error could be compounded. By ensuring that each device in the network uses the same clocking signal, you can ensure the integrity of the traffic.

If timing between devices is not maintained, a condition known as clock slip can occur. Clock slip is the repetition or deletion of a block of bits in a synchronous bit stream due to a discrepancy in the read and write rates at a buffer.

Slips are caused by the inability of an equipment buffer store (or other mechanisms) to accommodate differences between the phases or frequencies of the incoming and outgoing signals in cases where the timing of the outgoing signal is not derived from that of the incoming signal.

A T1 or E1 interface sends traffic inside repeating bit patterns called frames. Each frame is a fixed number of bits, allowing the device to see the start and end of a frame. The receiving device also knows exactly when to expect the end of a frame simply by counting the appropriate number of bits that have come in. Therefore, if the timing between the sending and receiving device is not the same, the receiving device may sample the bit stream at the wrong moment, resulting in an incorrect value being returned.

Even though Cisco IOS software can be used to control the clocking on these platforms, the default clocking mode is effectively free running, meaning that the received clock signal from an interface is not connected to the backplane of the router and used for internal synchronization between the rest of the router and its interfaces. The router will use its internal clock source to pass traffic across the backplane and other interfaces.

For data applications, this clocking generally does not present a problem as a packet is buffered in internal memory and is then copied to the transmit buffer of the destination interface. The reading and writing of packets to memory effectively removes the need for any clock synchronization between ports.

Digital voice ports have a different issue. It would appear that unless otherwise configured, Cisco IOS software uses the backplane (or internal) clocking to control the reading and writing of data to the digital signal processors (DSPs). If a PCM stream comes in on a digital voice port, it will obviously be using the external clocking for the received bit stream. However, this bit stream will not necessarily be using the same reference as the router backplane, meaning the DSPs will possibly misinterpret the data that is coming in from the controller.

This clocking mismatch is seen on the E1 or T1 controller of the router as a clock slip: The router is using its internal clock source to send the traffic out the interface, but the traffic coming in to the interface is using a completely different clock reference. Eventually, the difference in the timing relationship between the transmit and receive signal becomes so great that the controller registers a slip in the received frame.

To eliminate the problem, change the default clocking behavior through Cisco IOS configuration commands. It is *absolutely critical* to set up the clocking commands properly.

Even though these commands are optional, it is strongly recommended that you enter them as part of your configuration to ensure proper network clock synchronization.

network-clock-participate [**slot** *slot number* | **wic** *wic-slot* | **aim** *aim-slot-number*]
network-clock-select *priority* {**bri** | **t1** | **e1**} *slot*/*port*

The **network-clock-participate** command allows the router to use the clock from the line via the specified slot, WAN interface card (WIC), or advanced integration module (AIM) and synchronize the onboard clock to the same reference.

If multiple voice WICs (VWICs) are installed, the commands must be repeated for each installed card. The system clocking can be confirmed using the **show network clocks** command.

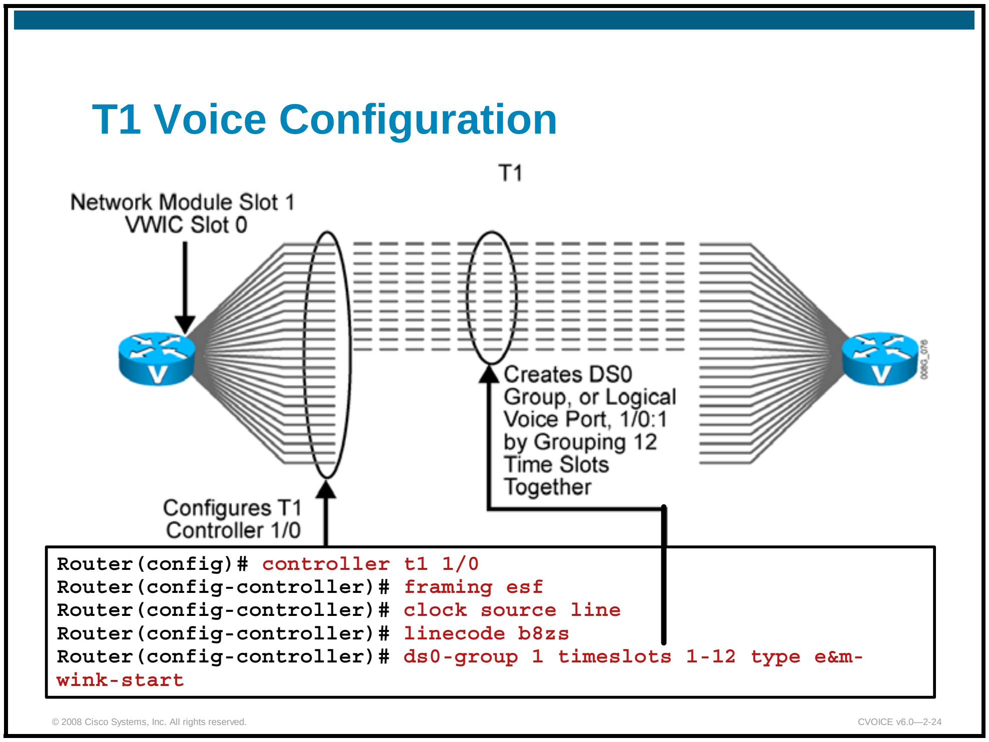
Caution If you are configuring Cisco 2600XM Series Multiservice Routers with an NM-HDV2 or NM-HD-2VE installed in slot 1, do not use the **network-clock-participate slot 1** command in the configuration. In this particular hardware scenario, the **network-clock-participate slot 1** command is not necessary. If the **network-clock-participate slot 1** command is configured, voice and data connectivity on interfaces terminating on the NM-HDV2 or NM-HD-2VE network module may fail to operate properly. Data connectivity to peer devices may not be possible at all, and even loopback plug tests to the serial interface spawned via a channel group configured on the local T1/E1 controller will fail. Voice groups such as CAS DS0 groups and ISDN PRI groups may fail to signal properly. The T1/E1 controller may accumulate large amounts of timing slips as well as Path Coding Violations (PCVs) and Line Coding Violations (LCVs).

DS0 Groups

For digital voice ports, a single command, **ds0-group**, performs the following functions:

- Defines the T1/E1 channels for compressed voice calls
- Automatically creates a logical voice port
- Defines the emulated analog signaling method that the router uses to connect to the PBX or PSTN

When you purchase a T1 or E1 connection, make sure that your service provider gives you the appropriate settings.



T1 Voice Configuration

T1

Network Module Slot 1
VWIC Slot 0

Creates DS0 Group, or Logical Voice Port, 1/0:1 by Grouping 12 Time Slots Together

Configures T1 Controller 1/0

```
Router(config)# controller t1 1/0
Router(config-controller)# framing esf
Router(config-controller)# clock source line
Router(config-controller)# linecode b8zs
Router(config-controller)# ds0-group 1 timeslots 1-12 type e&m-
wink-start
```

CVOICE v6.0—2-24

You must create a digital voice port on the T1 or controller to be able to configure voice port parameters. You must also assign time slots 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.

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

The *ds0-group-no* argument identifies the 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 time slots are part of the DS0 group. The *timeslot-list* argument 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.

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.

This figure shows how a **ds0-group** command gathers some of the DS0 time slots from a T1 line into a group that becomes a single logical voice port, which can later be addressed as a single entity in voice port configurations. Other DS0 groups for voice can be created from the remaining time slots shown in the figure, or the time slots can be used for data or serial pass-through.

T1 CAS Controller Configuration Example

In this example, you have been tasked to configure a T1 controller for a voice gateway according to the following network requirements.

- T1:
  - — Framing = ESF
  - — Line code = B8ZS
  - — Clock source = PSTN
  - — DS0 group = 1 will utilize 12 time slots with E&M wink-start signaling
- Voice port:
  - — Call progress tones = U.S.
  - — Companding standard = u-law

To configure controller settings for digital T1/E1 voice ports, use the following steps:

Step 1 Enter controller configuration mode.

```
Router(config)# controller {t1 | e1} slot/port
```

Step 2 Select frame type for T1 or E1 line.

- T1 lines:

```
Router(config-controller)# framing {sf | esf}
```

- E1 lines:

```
Router(config-controller)# framing {crc4 | no-crc4}
[Australia]
```

Use this command in configurations in which the router or access server is intended to communicate with T1 or E1 fractional data lines. The service provider determines the framing type that is required for your T1/E1 circuit.

This command does not have a **no** form.

Step 3 Configure the clock source.

```
Router(config-controller)# clock source {line [primary | bits]
| internal | free-running}
```

The **line** keyword specifies that the clock source is derived from the active line rather than from the free-running internal clock. The following rules apply to clock sourcing on the controller ports:

- When both ports are set to line clocking with no primary specification, port 0 is the default primary clock source and port 1 is the default secondary clock source.
- When both ports are set to line and one port is set as the primary clock source, the other port is by default the backup or secondary source and is loop-timed.
- If one port is set to clock source line or clock source line primary and the other is set to clock source internal, the internal port recovers clock from the clock source line port if the clock source line port is up. If it is down, then the internal port generates its own clock.
- If both ports are set to clock source internal, there is only one clock source: internal.

Step 4 Specify the line encoding to use.

- T1 lines:

```
Router(config-controller)# linecode {ami | b8zs}
```

- E1 lines:

```
Router(config-controller)# linecode {ami | hdb3}
```

Use this command in configurations in which the router or access server must communicate with T1 fractional data lines. The T1 service provider determines which line code type, either **ami** or **b8zs**, is required for your T1 circuit. Likewise, the E1 service provider determines which line code type, either **ami** or **hdb3**, is required for your E1 circuit.

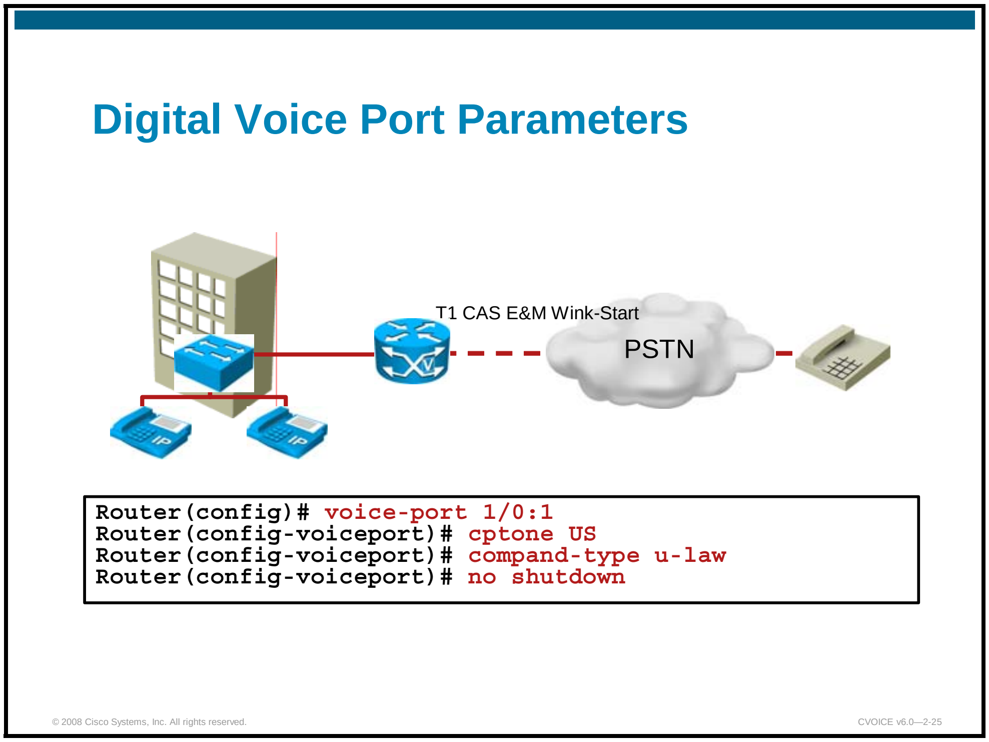
Step 5 Define the T1 channels for use by compressed voice calls and the signaling method that the router uses to connect to the PBX or CO.

```
Router(config-controller)# ds0-group ds0-group-number
timeslots timeslot-list [service service-type] type {e&m-fgb |
e&m-fgd | e&m-immediate-start | fgd-eana | fgd-os | fxs-
ground-start | fxs-loop-start | none | r1-itu | r1-modified |
r1-turkey}
```

The **ds0-group** command automatically creates a logical voice port. The resulting logical voice port will be 1/0:1, where 1/0 is the module and slot number and :1 is the *ds0-group-number* argument that you will assign in this step.

Step 6 Activate the controller.

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



Digital Voice Port Parameters

```
Router(config)# voice-port 1/0:1
Router(config-voiceport)# cptone US
Router(config-voiceport)# compand-type u-law
Router(config-voiceport)# no shutdown
```

CVOICE v6.0—2-25

After setting up the controller, you can now configure voice port parameters for that digital voice port. When you specified a **ds0-group**, the system automatically created a logical voice port. You must then enter the voice-port configuration mode to configure port-specific parameters. Each voice port that you set up in digital voice port configuration is one of the logical voice ports that you created with the **ds0-group** command.

Follow these steps to configure basic parameters for digital T1/E1 voice ports:

Step 1 Enter voice-port configuration mode.

```
Router(config)# voice-port slot/port:ds0-group-number
```

Step 2 Select a two-letter keyword for the voice call progress tones and other locale-specific parameters to be used on this voice port.

```
Router(config -voiceport)# cptone locale
```

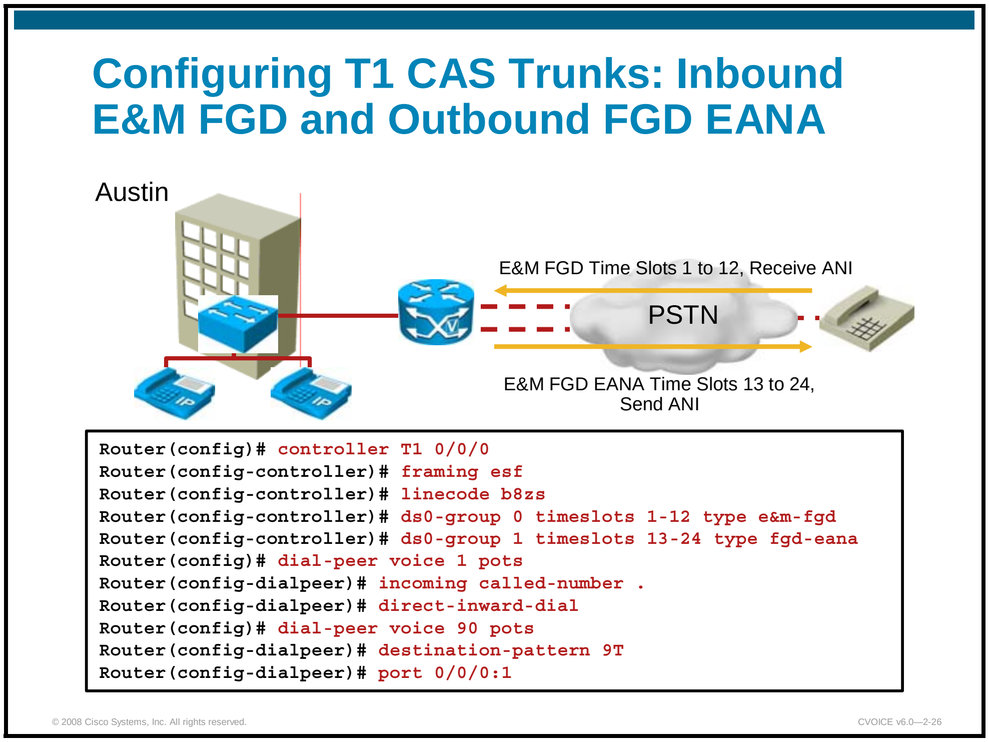
Step 3 Specify the companding standard that is used to convert between analog and digital signals.

```
Router(config -voiceport)# compand-type {u-law | a-law}
```

Note This command is used in cases when the DSP is not used, such as local cross-connects, and overwrites the **compand-type** value set by the **cptone** command.

Step 4 Activate the voice port.

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



Configuring T1 CAS Trunks: Inbound E&M FGD and Outbound FGD EANA

Austin
E&M FGD Time Slots 1 to 12, Receive ANI
PSTN
E&M FGD EANA Time Slots 13 to 24,
Send ANI

```
Router(config)# controller T1 0/0/0
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# ds0-group 0 timeslots 1-12 type e&m-fgd
Router(config-controller)# ds0-group 1 timeslots 13-24 type fgd-eana
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer)# incoming called-number .
Router(config-dialpeer)# direct-inward-dial
Router(config)# dial-peer voice 90 pots
Router(config-dialpeer)# destination-pattern 9T
Router(config-dialpeer)# port 0/0/0:1
```

CVOICE v6.0—2-26

Because E&M FGD supports only inbound ANI, a deployment requiring both inbound and outbound ANI can combine an E&M FGD and FGD-EANA trunk. The FGD trunk will be used for inbound calls, and the FGD-EANA trunk will be used for outbound calls.

T1 CAS with E&M FGD and FGD-EANA Trunk Configuration Example

In this example, you have been tasked to configure an E1 controller for a voice gateway according to the following network requirements.

- E1:
  - Framing = ESF.
  - Line code = B8ZS.
  - Time slots 1 to 12 should be the FGD trunk.
  - Time slots 13 to 24 should be the FGD-EANA trunk.
- The voice gateway must support inbound and outbound ANI.

Follow this procedure to configure a T1 CAS digital voice port with inbound and outbound ANI.

Step 1 Enter controller configuration mode.

```
Router(config)# controller T1 0/0/0
```

Step 2 Specify the framing format.

```
Router(config-controller)# framing esf
```

Step 3 Specify the line coding.

```
Router(config-controller)# linecode b8zs
```

Step 4 Configure one DS0 group to use time slots 1 to 12 and E&M FGD.

```
Router(config-controller)# ds0-group 0 timeslots 1-12 type
e&m-fgd
```

Step 5 Configure another DS0 group to use time slots 13 to 24 and E&M FGD-EANA.

```
Router(config-controller)# ds0-group 1 timeslots 13-24 type
fgd-eana
```

Note This configuration creates two voice ports, 0/0/0:0 and 0/0/0:1

Step 6 An inbound dial peer is configured using the 0/0/0:0 trunk, which supports inbound ANI.

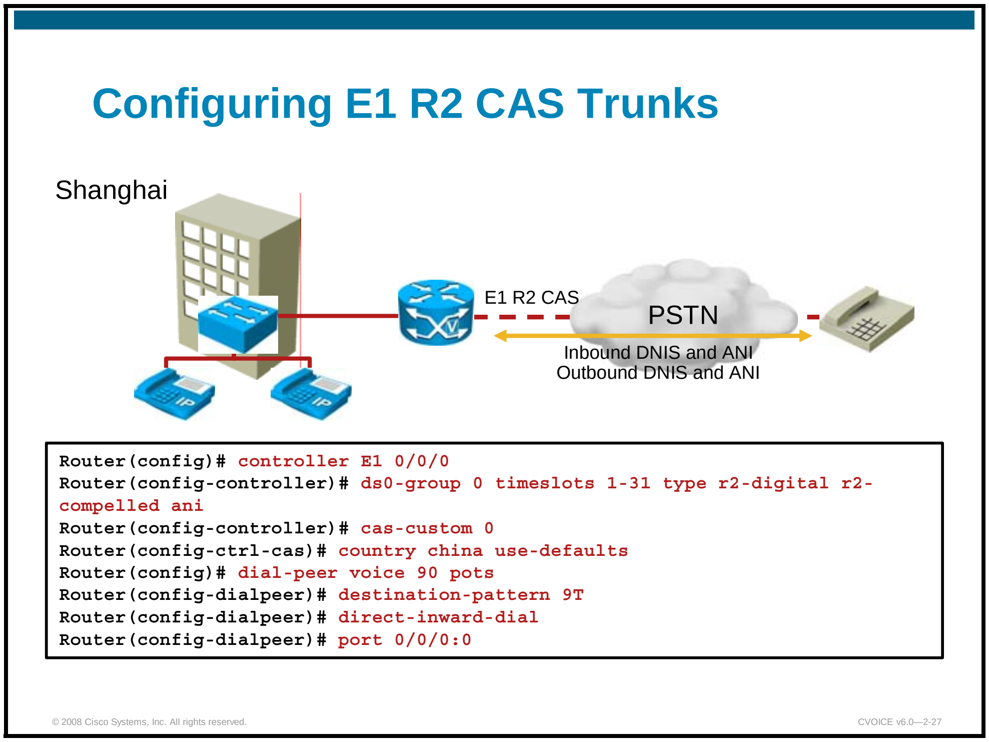
```
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer)# incoming called-number .
Router(config-dialpeer)# port 0/0/0:0
```

Step 7 An outbound dial peer is configured using the 0/0/0:1 trunk, which supports outbound ANI.

```
Router(config)# dial-peer voice 90 pots
Router(config-dialpeer)# destination-pattern 9T
Router(config-dialpeer)# port 0/0/0:1
```

Configuring E1 R2 CAS Trunks

This topic describes how to configure E1 R2 CAS trunks.



Configuring E1 R2 CAS Trunks

```
Router(config)# controller E1 0/0/0
Router(config-controller)# ds0-group 0 timeslots 1-31 type r2-digital r2-
compelled ani
Router(config-controller)# cas-custom 0
Router(config-ctrl-cas)# country china use-defaults
Router(config)# dial-peer voice 90 pots
Router(config-dialpeer)# destination-pattern 9T
Router(config-dialpeer)# direct-inward-dial
Router(config-dialpeer)# port 0/0/0:0
```

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-27

You use the **ds0-group** controller command to configure E1 R2 trunks also. The Cisco implementation of R2 signaling has DNIS support enabled by default. If you enable the ANI option, DNIS information is still collected. Specification of the ANI option does not disable the DNIS collection.

T1 CAS with E&M FGD and EANA FGD Trunk Configuration Example

In this example, you have been tasked to configure an E1 controller for a voice gateway according to the following network requirements.

- E1:
  - Framing = ESF.
  - Line code = B8ZS.
  - Time slots 1 to 31 should use R2 digital signaling.
- The voice gateway must support inbound and outbound DNIS and ANI.

Follow this procedure to configure a T1 CAS digital voice port with inbound and outbound ANI.

Step 1 Enter controller configuration mode.

```
Router(config)# controller E1 0/0/0
```

Step 2 Define DS0 groups.

```
Router(config-controller)# ds0-group 0 timeslots 1-31 type r2-
digital r2-compelled ani
```

After the DS0 group has been created, you can tune additional parameters using the **cas custom** *ds0-id* command.

Step 3 Customize E1 R2 signaling parameters.

```
Router(config-controller)# cas-custom 0
```

Use the other **cas-custom** subcommands for further customization that is required to accommodate a certain PBX or switch.

```
Router(config-ctrl-cas)# country china use-defaults
```

Use this command to specify the local country, regional, and some corporation settings for R2 signaling. Replace the *name* variable with one of the supported country names. The default country setting is ITU.

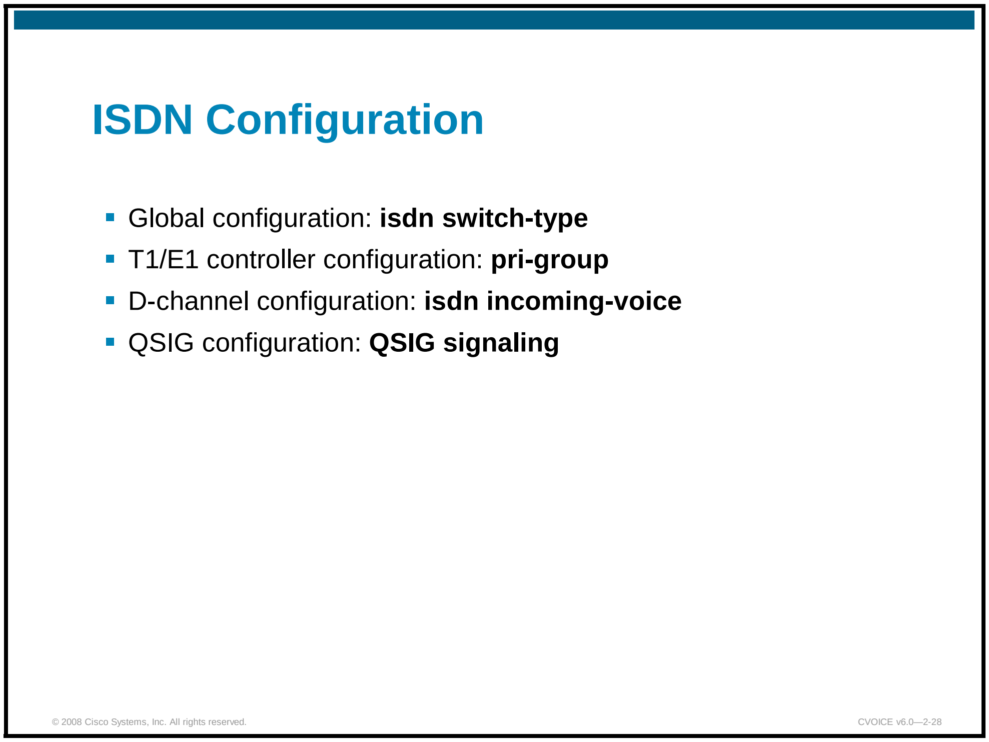
Note Cisco strongly recommends that you include the **use-defaults** option, which enables the default settings for a specific country.

Step 4 Create a dial peer.

```
Router(config)# dial-peer voice 90 pots
Router(config-dialpeer)# destination-pattern 9T
Router(config-dialpeer)# port 0/0/0:0
Router(config-dialpeer)# direct-inward-dial
```

Configuring ISDN Trunks

This topic describes how to configure and verify BRI and PRI trunks to the PSTN.



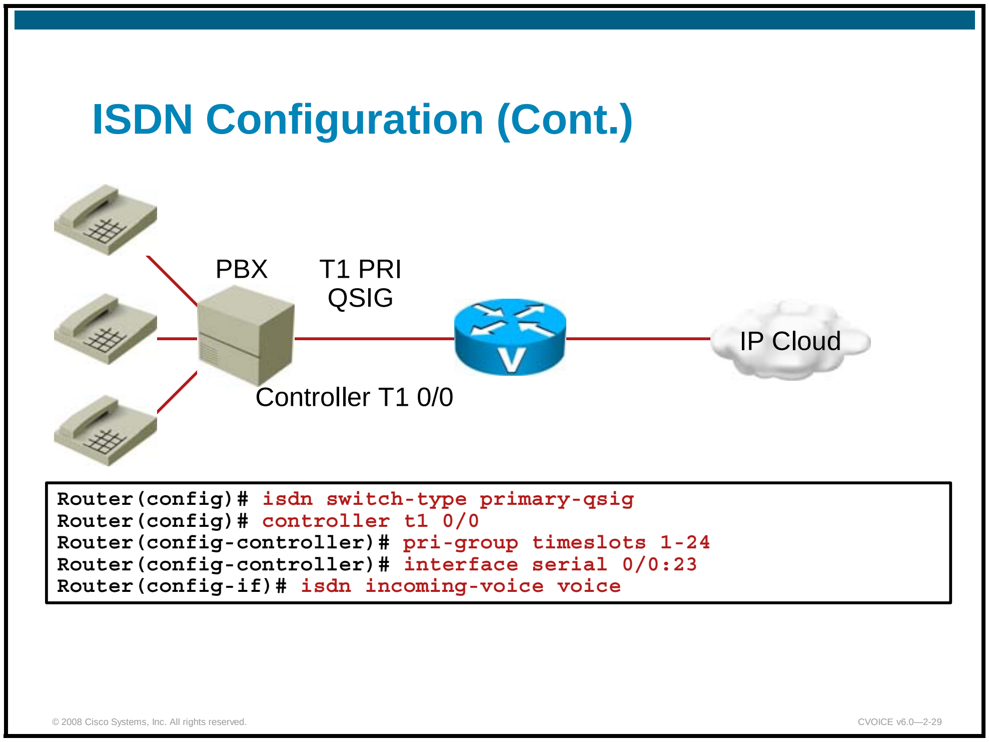
ISDN Configuration

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

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-28

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

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



ISDN Configuration (Cont.)

```
Router(config)# isdn switch-type primary-qsig
Router(config)# controller t1 0/0
Router(config-controller)# pri-group timeslots 1-24
Router(config-controller)# interface serial 0/0:23
Router(config-if)# isdn incoming-voice voice
```

CVOICE v6.0—2-29

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

Follow these steps to configure an ISDN voice port:

Step 1 Specify the CO switch type on the ISDN interface.

```
Router(config)# isdn switch-type primary-qsig
```

You have a choice of configuring the **isdn-switch-type** command to support QSIG at either the global configuration level or at the interface configuration level.

Step 2 Enter controller configuration mode.

```
Router(config)# controller t1 0/0
```

Step 3 Specify an ISDN PRI group.

```
Router(config-controller)# pri-group timeslots 1-24
```

Step 4 Enter voice-port configuration mode.

```
Router(config)# interface serial 0/0:23
```

Step 5 Send incoming calls to DSPs.

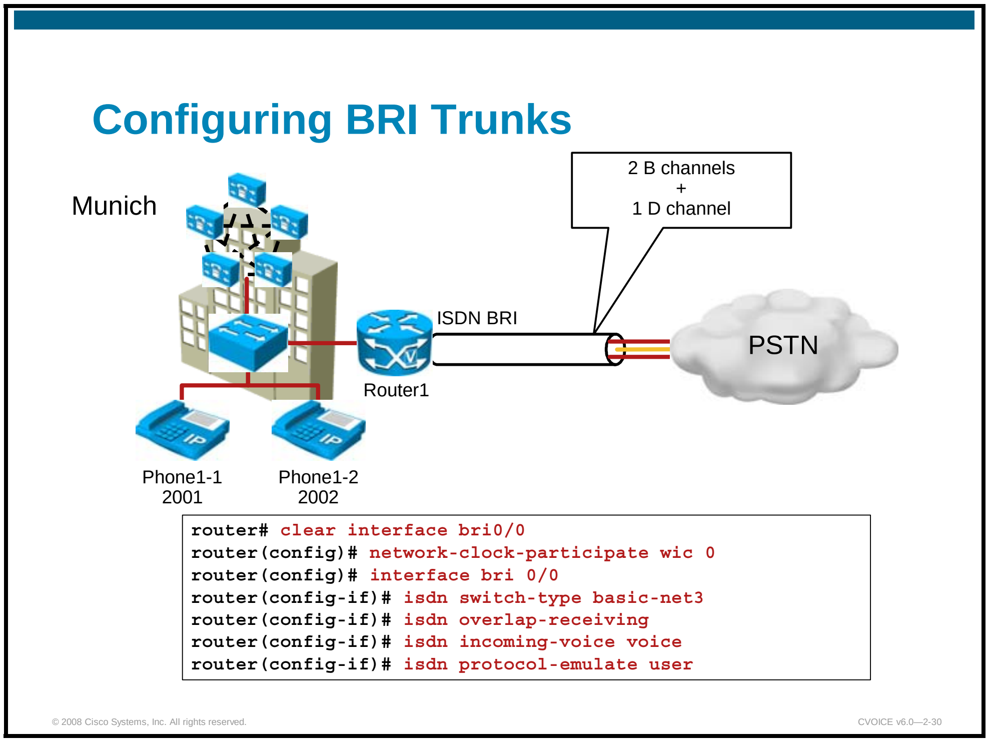
```
Router(config-if)# isdn incoming-voice voice
```

Step 6 Activate the voice port.

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

Configuring a BRI Trunk Example

This subtopic describes how to configure a BRI trunk to the PSTN.



Configuring BRI Trunks

```
router# clear interface bri0/0
router(config)# network-clock-participate wic 0
router(config)# interface bri 0/0
router(config-if)# isdn switch-type basic-net3
router(config-if)# isdn overlap-receiving
router(config-if)# isdn incoming-voice voice
router(config-if)# isdn protocol-emulate user
```

In this scenario, Router1 will be configured with a BRI connection to the PSTN, providing two B channels and one D channel.

BRI Trunk Configuration Example

In this example, you have been tasked to configure a BRI connection to the PSTN according to the following network requirements.

- Because the ISDN switch is located in Munich, you need to configure the ISDN switch type as **basic-net3** for Germany.
- The DSP clocking will be synchronized with the WIC in slot 0.
- Because there is the possibility of the incoming number being sent digit-by-digit and not *en bloc*, you need to configure **isdn overlap-receiving**.
- To define incoming calls as voice-only, configure **isdn incoming-voice voice**. This configuration will send incoming calls to the DSP resources.
- If the current configuration is set to network-side, use the **isdn protocol-emulate user** command to switch to user-side ISDN. The user-side setting is the default so it is not shown in the configuration.

Perform these steps to build the BRI trunk to the PSTN:

Step 1 Configure DSP clocking so it is synchronized with the PSTN clock.

Step 2 Configure the ISDN switch type according to the country ISDN implementation.

Step 3 Configure ISDN overlap-receiving for countries with variable-length numbering plans.

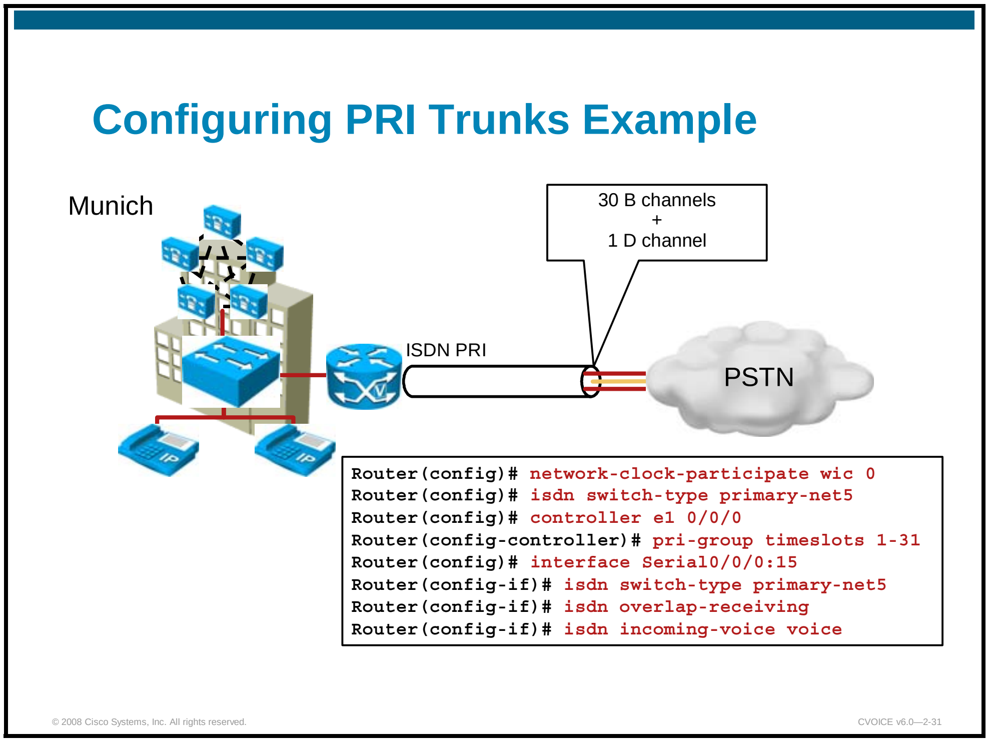
Step 4 Configure incoming ISDN calls as voice. The calls will be directly passed to the DSPs.

Step 5 Configure BRI as user side, if necessary. This is the default, so it does not need to be configured under most circumstances.

Step 6 Reset the interface if necessary, depending on the configuration.

Configuring PRI Trunks Example

This subtopic describes how to configure a PRI trunk to the PSTN.



Configuring PRI Trunks Example

```
Router(config)# network-clock-participate wic 0
Router(config)# isdn switch-type primary-net5
Router(config)# controller e1 0/0/0
Router(config-controller)# pri-group timeslots 1-31
Router(config)# interface Serial0/0/0:15
Router(config-if)# isdn switch-type primary-net5
Router(config-if)# isdn overlap-receiving
Router(config-if)# isdn incoming-voice voice
```

In this scenario, Router1 will be configured with a PRI connection to the PSTN, providing 30 B channels and 1 D channel.

PRI Trunk Configuration Example

In this example, you have been tasked to configure a PRI connection to the PSTN according to the following network requirements.

- The ISDN switch is located in Munich, Germany. According to the “ISDN Switch Type BRI Parameters” table, you need to configure the ISDN switch type as **primary-net5**.
- The DSP clocking will be synchronized with the WIC in slot 0.
- The line coding needs to be defined for the E1 controller. In this case, use **linecoding ami**. This is not shown in the figure because this is the default configuration.
- The framing needs to be defined for the E1 controller. In this case, use **crc4 framing**. This is not shown in the figure because this is the default configuration.
- The clock source will be set to the PSTN. This is the default setting, so it is not shown in the configuration.
- The logical voice ports need to be created. This is done with the **pri-group timeslots 1-31** command, which defines all 30 B channels as logical voice ports. This is not shown in the figure because this is the default configuration.
- A variable-length numbering plan needs to be configured. Although the users have a four-digit extension, the switchboard is available via a “0” extension. You therefore configure overlap-receiving.

- To define incoming calls as voice-only, you configure **isdn incoming-voice voice**. This will send incoming calls to the DSP resources.

Perform these steps to build the PRI trunk to the PSTN:

Step 1 Configure the ISDN switch type according to the country ISDN implementation.

Step 2 Configure DSP clocking so it is synchronized with the PSTN clock.

Step 3 Configure the E1 line code. Refer to the local service provider for the correct setting.

Step 4 Configure the E1 frame format. Refer to the local service provider for the correct setting.

Step 5 Configure the clock source to define which side will provide clocking.

Step 6 Configure a logical voice port to define which channels will be used for voice.

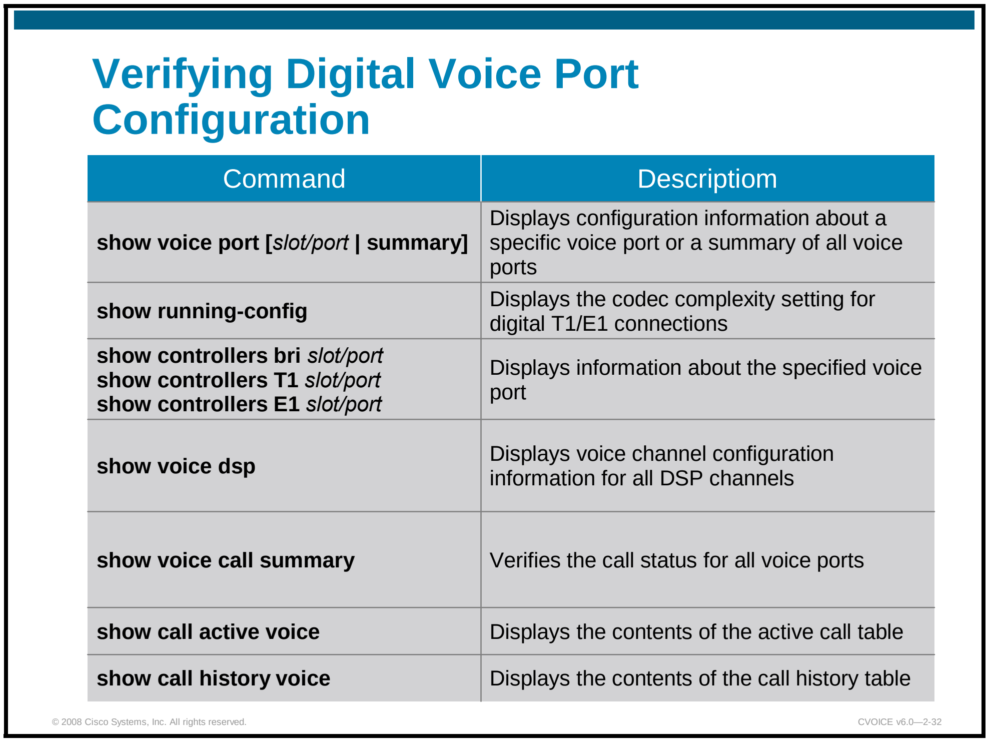
Step 7 Configure ISDN overlap-receiving for countries with variable-length numbering plans.

Step 8 Configure incoming ISDN calls as voice. The calls will be directly passed to the DSPs.

Step 9 Reset the interface if necessary, depending on the configuration.

Verifying Digital Voice Ports

This topic describes how to verify a digital voice port.



Verifying Digital Voice Port Configuration

Command	Descriptiom
show voice port [*slot/port* **| summary]**	Displays configuration information about a specific voice port or a summary of all voice ports
show running-config	Displays the codec complexity setting for digital T1/E1 connections
show controllers bri *slot/port* **show controllers T1** *slot/port* **show controllers E1** *slot/port*	Displays information about the specified voice port
show voice dsp	Displays voice channel configuration information for all DSP channels
show voice call summary	Verifies the call status for all voice ports
show call active voice	Displays the contents of the active call table
show call history voice	Displays the contents of the call history table

CVOICE v6.0—2-32

After you have configured the voice ports on your router, perform the following steps to verify proper operation.

Step 1 Pick up the handset of an attached telephony device and check for a dial tone.

Step 2 If you have dial tone, check for DTMF detection. If the dial tone stops when you dial a digit, then the voice port is probably configured properly.

Step 3 Use the **show voice port summary** command to identify the port numbers of voice interfaces installed in your router.

Step 4 Use the **show voice port** command to verify voice port parameter settings.

Step 5 Use the **show running-config** command to verify the codec complexity setting for digital T1/E1 connections.

Step 6 Use the **show controller** command to verify that the digital T1/E1 controller is up and that no alarms have been reported, and to display information about clock sources and other controller settings.

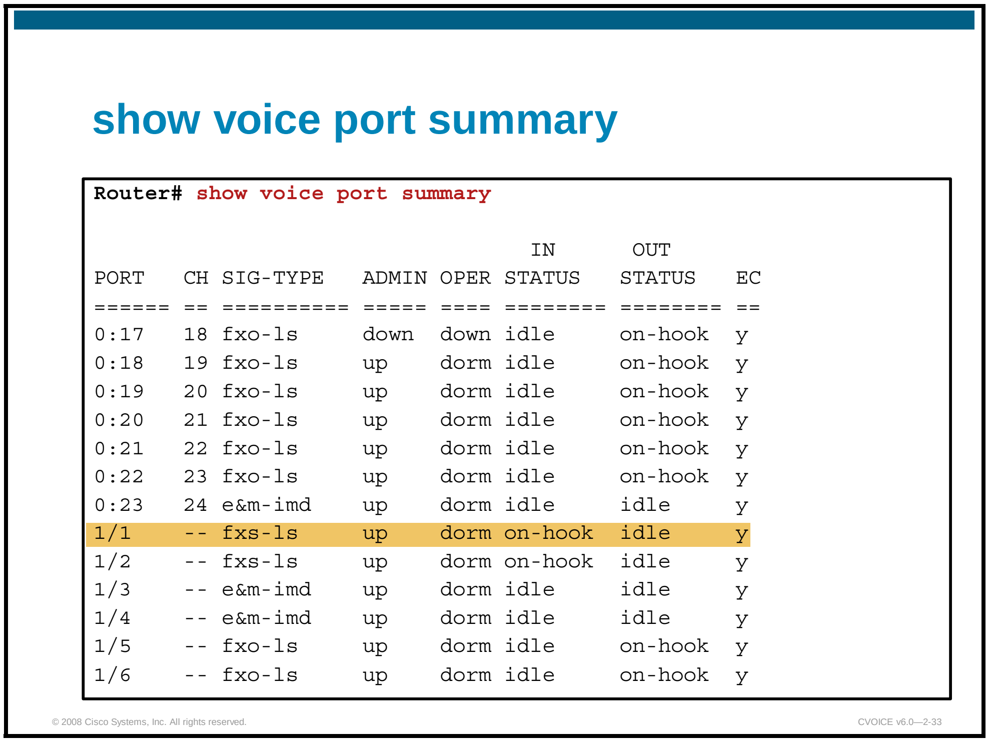
Step 7 Use the **show voice dsp** command to display voice channel configuration information for all DSP channels.

Step 8 Use the **show voice call summary** command to verify the call status for all voice ports.

Step 9 Use the **show call active voice** command to display the contents of the active call table, which shows all of the calls currently connected through the router or concentrator.

Step 10 Use the **show call history voice** command to display the contents of the call history table.

Following are some examples of commands that are used to verify digital port configurations.

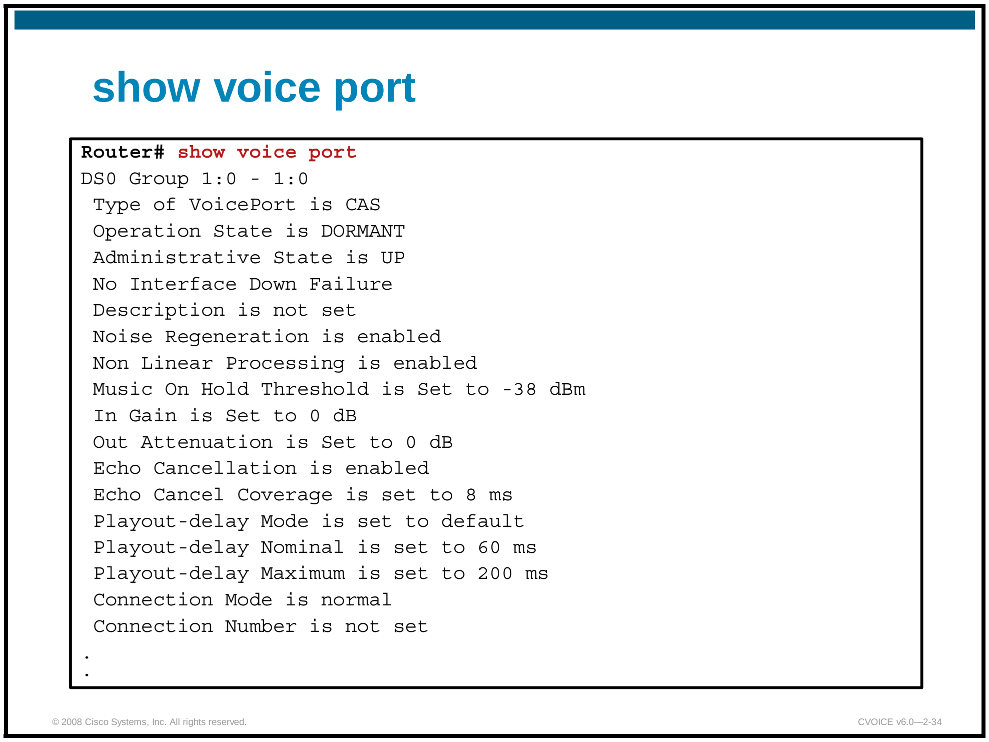


show voice port summary

```
Router# show voice port summary

                                       IN       OUT
PORT   CH SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
====== == ========== ===== ==== ======== ======== ==
0:17   18 fxo-ls     down  down idle     on-hook  y
0:18   19 fxo-ls     up    dorm idle     on-hook  y
0:19   20 fxo-ls     up    dorm idle     on-hook  y
0:20   21 fxo-ls     up    dorm idle     on-hook  y
0:21   22 fxo-ls     up    dorm idle     on-hook  y
0:22   23 fxo-ls     up    dorm idle     on-hook  y
0:23   24 e&m-imd    up    dorm idle     idle     y
1/1    -- fxs-ls     up    dorm on-hook  idle     y
1/2    -- fxs-ls     up    dorm on-hook  idle     y
1/3    -- e&m-imd    up    dorm idle     idle     y
1/4    -- e&m-imd    up    dorm idle     idle     y
1/5    -- fxo-ls     up    dorm idle     on-hook  y
1/6    -- fxo-ls     up    dorm idle     on-hook  y
```

CVOICE v6.0—2-33

The diagram shows the output of the **show voice port summary c**ommand. This figure shows the status of an FXS port.

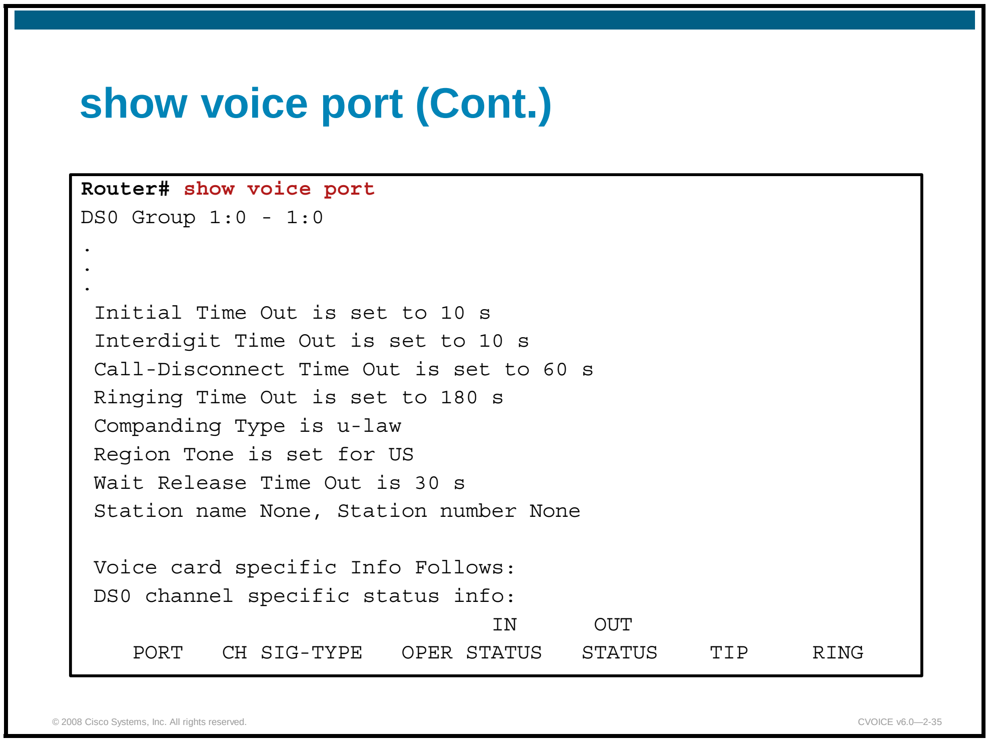


show voice port

```
Router# show voice port
DS0 Group 1:0 - 1:0
 Type of VoicePort is CAS
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 8 ms
 Playout-delay Mode is set to default
 Playout-delay Nominal is set to 60 ms
 Playout-delay Maximum is set to 200 ms
 Connection Mode is normal
 Connection Number is not set
.
.
```

CVOICE v6.0—2-34

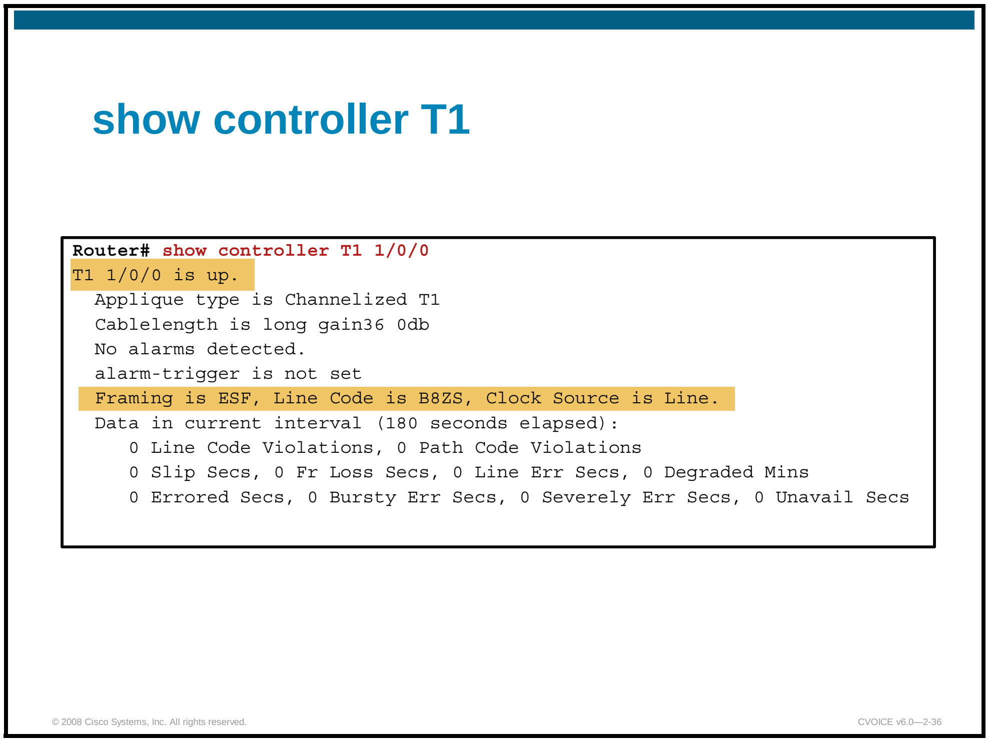
These diagrams show the output of the **show voice port** command.



show voice port (Cont.)

```
Router# show voice port
DS0 Group 1:0 - 1:0
.
.
.
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Call-Disconnect Time Out is set to 60 s
 Ringing Time Out is set to 180 s
 Companding Type is u-law
 Region Tone is set for US
 Wait Release Time Out is 30 s
 Station name None, Station number None

 Voice card specific Info Follows:
 DS0 channel specific status info:
                                IN      OUT
    PORT   CH SIG-TYPE   OPER STATUS   STATUS    TIP     RING
```

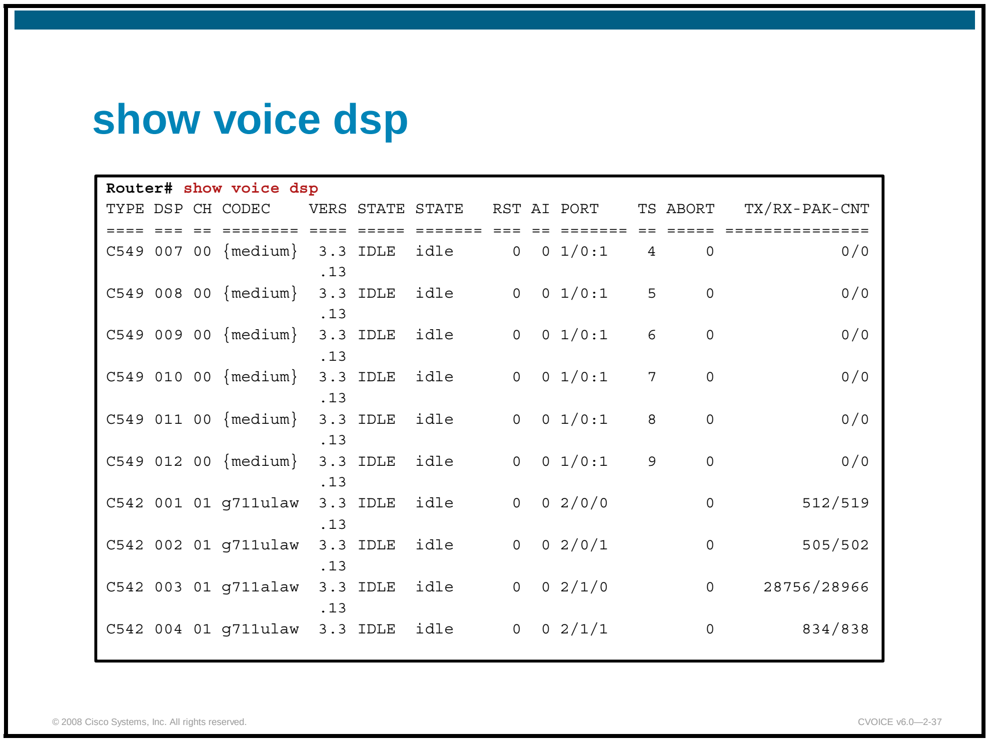
CVOICE v6.0—2-35



show controller T1

```
Router# show controller T1 1/0/0
T1 1/0/0 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  Data in current interval (180 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

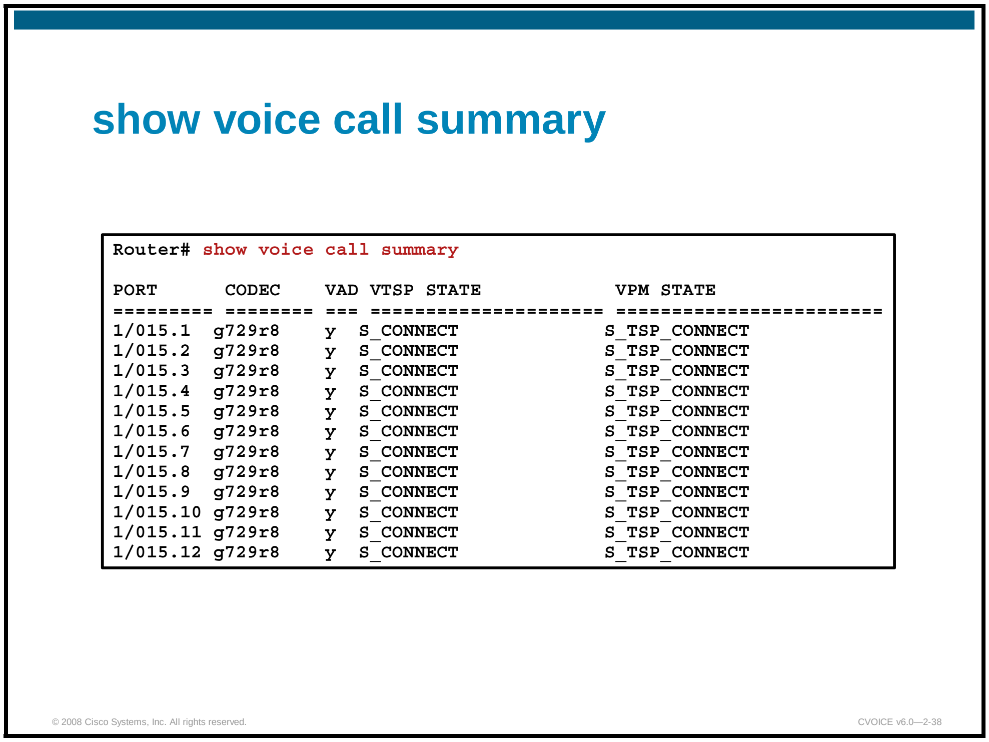
The figure shows the output of the **show controller T1** command. You can use this command to verify operation of the controller in addition to correct framing, line code, and clock source.



show voice dsp

```
Router# show voice dsp
TYPE DSP CH CODEC    VERS STATE STATE   RST AI PORT    TS ABORT   TX/RX-PAK-CNT
==== === == ======== ==== ===== ======= === == ======= == ===== ===============
C549 007 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    4     0             0/0
                      .13
C549 008 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    5     0             0/0
                      .13
C549 009 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    6     0             0/0
                      .13
C549 010 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    7     0             0/0
                      .13
C549 011 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    8     0             0/0
                      .13
C549 012 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    9     0             0/0
                      .13
C542 001 01 g711ulaw  3.3 IDLE  idle      0  0 2/0/0          0         512/519
                      .13
C542 002 01 g711ulaw  3.3 IDLE  idle      0  0 2/0/1          0         505/502
                      .13
C542 003 01 g711alaw  3.3 IDLE  idle      0  0 2/1/0          0     28756/28966
                      .13
C542 004 01 g711ulaw  3.3 IDLE  idle      0  0 2/1/1          0         834/838
```

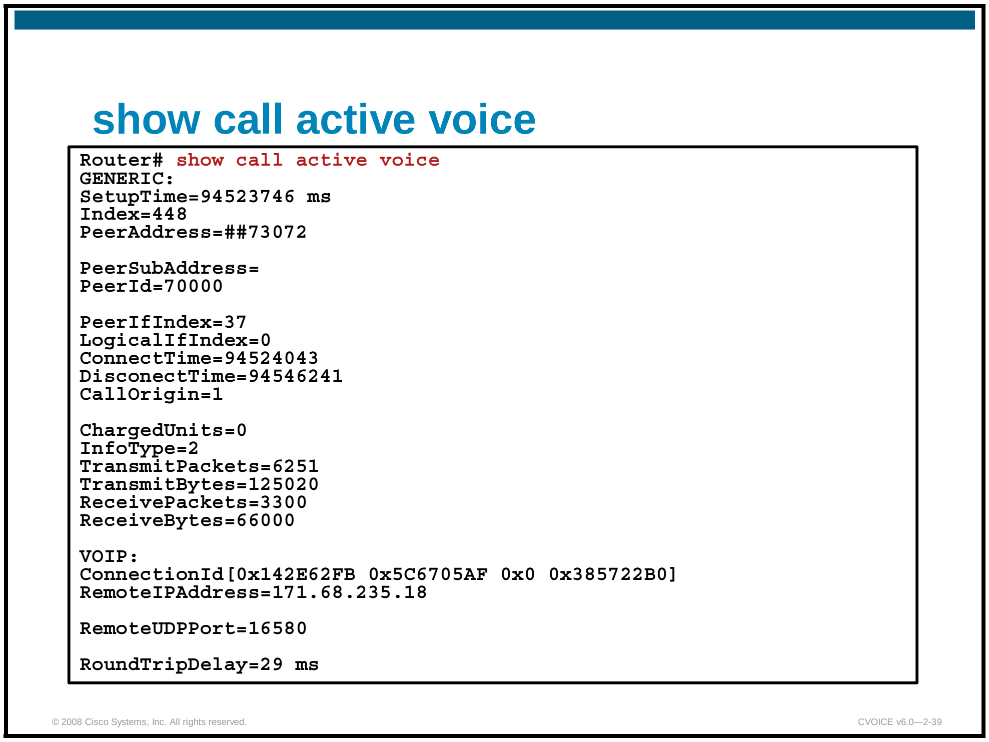
The figure shows the output of the **show voice dsp** command.



show voice call summary

```
Router# show voice call summary

PORT      CODEC    VAD VTSP STATE            VPM STATE
========= ======== === ===================== ========================
1/015.1  g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.2  g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.3  g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.4  g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.5  g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.6  g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.7  g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.8  g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.9  g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.10 g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.11 g729r8    y  S_CONNECT             S_TSP_CONNECT
1/015.12 g729r8    y  S_CONNECT             S_TSP_CONNECT
```

The figure shows the output of the **show voice call summary** command.

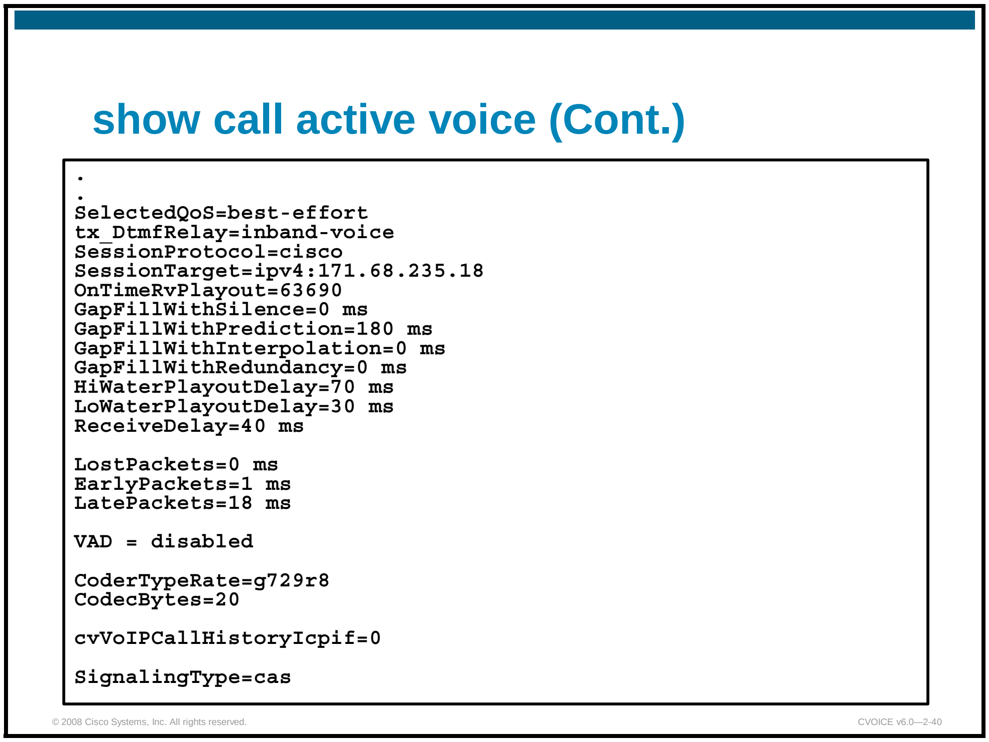


show call active voice

```
Router# show call active voice
GENERIC:
SetupTime=94523746 ms
Index=448
PeerAddress=##73072

PeerSubAddress=
PeerId=70000

PeerIfIndex=37
LogicalIfIndex=0
ConnectTime=94524043
DisconectTime=94546241
CallOrigin=1

ChargedUnits=0
InfoType=2
TransmitPackets=6251
TransmitBytes=125020
ReceivePackets=3300
ReceiveBytes=66000

VOIP:
ConnectionId[0x142E62FB 0x5C6705AF 0x0 0x385722B0]
RemoteIPAddress=171.68.235.18

RemoteUDPPort=16580

RoundTripDelay=29 ms
```

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-39

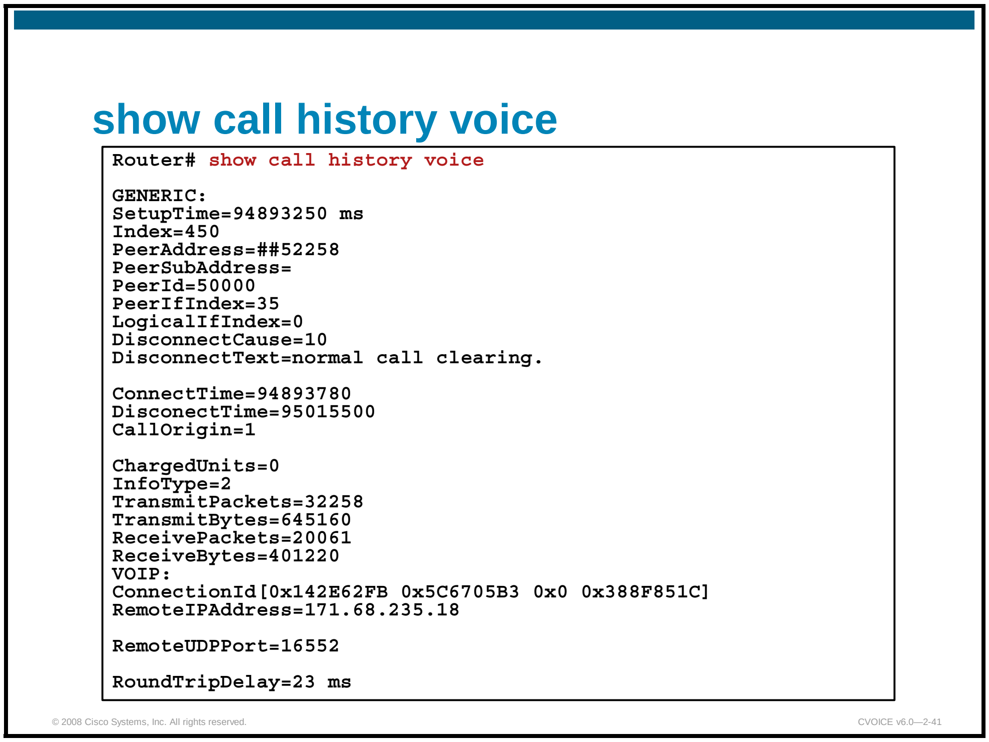
These figures show the output of the **show call active voice** command.



show call active voice (Cont.)

```
.
.
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
SessionProtocol=cisco
SessionTarget=ipv4:171.68.235.18
OnTimeRvPlayout=63690
GapFillWithSilence=0 ms
GapFillWithPrediction=180 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=30 ms
ReceiveDelay=40 ms

LostPackets=0 ms
EarlyPackets=1 ms
LatePackets=18 ms

VAD = disabled

CoderTypeRate=g729r8
CodecBytes=20

cvVoIPCallHistoryIcpif=0

SignalingType=cas
```

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-40

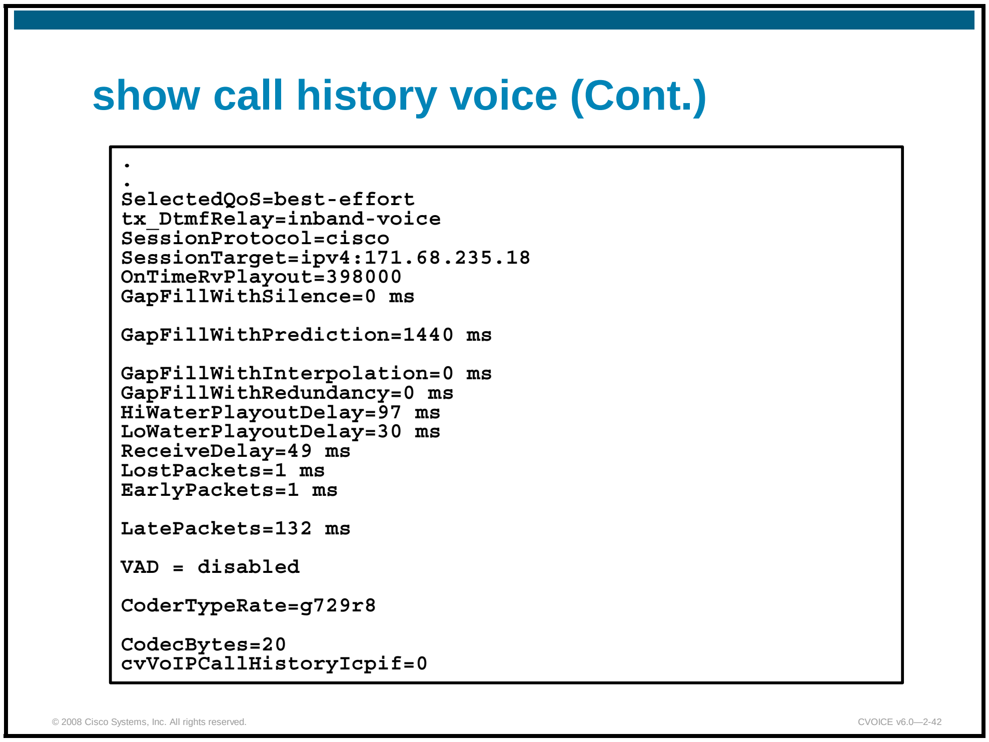


show call history voice

```
Router# show call history voice

GENERIC:
SetupTime=94893250 ms
Index=450
PeerAddress=##52258
PeerSubAddress=
PeerId=50000
PeerIfIndex=35
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing.

ConnectTime=94893780
DisconectTime=95015500
CallOrigin=1

ChargedUnits=0
InfoType=2
TransmitPackets=32258
TransmitBytes=645160
ReceivePackets=20061
ReceiveBytes=401220
VOIP:
ConnectionId[0x142E62FB 0x5C6705B3 0x0 0x388F851C]
RemoteIPAddress=171.68.235.18

RemoteUDPPort=16552

RoundTripDelay=23 ms
```

CVOICE v6.0—2-41

These figures show the output of the **show call history voice** command.



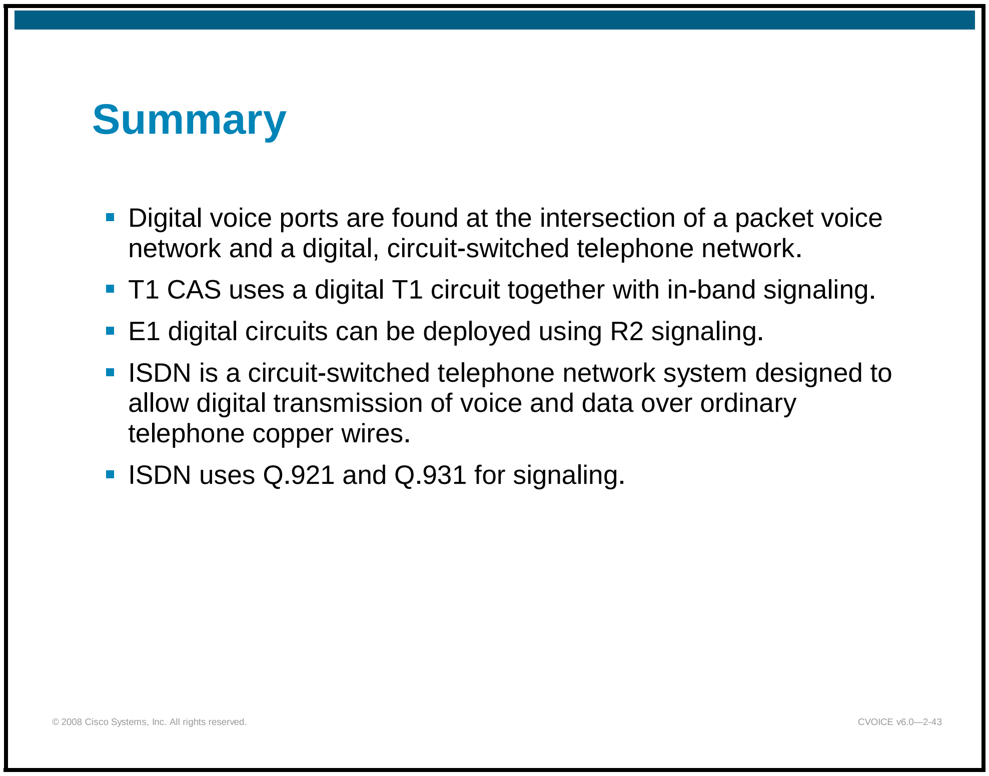
show call history voice (Cont.)

```
.
.
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
SessionProtocol=cisco
SessionTarget=ipv4:171.68.235.18
OnTimeRvPlayout=398000
GapFillWithSilence=0 ms

GapFillWithPrediction=1440 ms

GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=97 ms
LoWaterPlayoutDelay=30 ms
ReceiveDelay=49 ms
LostPackets=1 ms
EarlyPackets=1 ms

LatePackets=132 ms

VAD = disabled

CoderTypeRate=g729r8

CodecBytes=20
cvVoIPCallHistoryIcpif=0
```

CVOICE v6.0—2-42

Summary

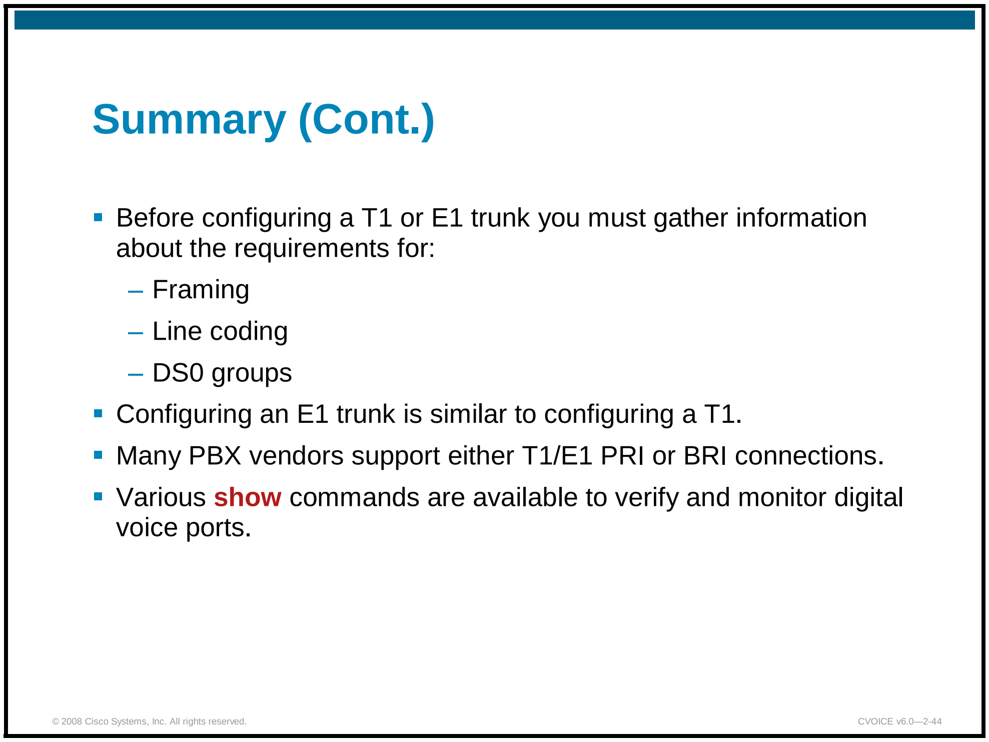
This topic summarizes the key points that were discussed in this lesson.



Summary

- Digital voice ports are found at the intersection of a packet voice network and a digital, circuit-switched telephone network.
- T1 CAS uses a digital T1 circuit together with in-band signaling.
- E1 digital circuits can be deployed using R2 signaling.
- ISDN is a circuit-switched telephone network system designed to allow digital transmission of voice and data over ordinary telephone copper wires.
- ISDN uses Q.921 and Q.931 for signaling.

CVOICE v6.0—2-43



Summary (Cont.)

- Before configuring a T1 or E1 trunk you must gather information about the requirements for:
  - Framing
  - Line coding
  - DS0 groups
- Configuring an E1 trunk is similar to configuring a T1.
- Many PBX vendors support either T1/E1 PRI or BRI connections.
- Various **show** commands are available to verify and monitor digital voice ports.

CVOICE v6.0—2-44

Lesson Self-Check

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

Q1) What are the three types of digital voice ports? (Choose three.)

Relates to: Digital Voice Ports

A) ISDN
B) PPP
C) E1
D) T1
E) analog
F) digital

Q2) T1 CAS uses _____ signaling.

Relates to: T1 CAS

A) wink-start
B) loop-start
C) robbed-bit
D) ground-start

Q3) When E1 R2 is being used, time slot _____ is used for signaling, and each of its frames carries information for _____ voice time slots.

Relates to: E1 R2 CAS

A) 16, three
B) 16, two
C) 17, three
D) 17, two

Q4) The _____ command is used to configure an E1 controller as an E1 R2 CAS interface.

Relates to: E1 R2 CAS

A) **type r2-digital**
B) **trunk r2-digital**
C) **type r2**
D) **trunk r2**

Q5) The two types of ISDN interfaces are _____ and _____.

Relates to: ISDN

A) T1, E1
B) PRI, BRI
C) T1, PRI
D) E1, BRI

Q6) ISDN uses _____ for Layer 2 signaling, which is defined in _____.

Relates to: ISDN Signaling

A) LAPB, Q.931
B) LAPD, Q.931
C) LAPB, Q.921
D) LAPD, Q.921

Q7) The _____ command is used to configure a T1 controller for CAS.

Relates to: Configuring a T1 CAS Trunk

A) **pri-group**
B) **bri-group**
C) **ds0-group**
D) **ds1-group**

Lesson Self-Check Answer Key

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

Lesson 5

Understanding QSIG

Overview

Q Signaling (QSIG) is an extension of ISDN and supports enterprise-class call features, such as signaling Message Waiting Indicators (MWIs) and call back. This lesson describes the characteristics of the QSIG and how to implement QSIG trunks on a Cisco IOS gateway.

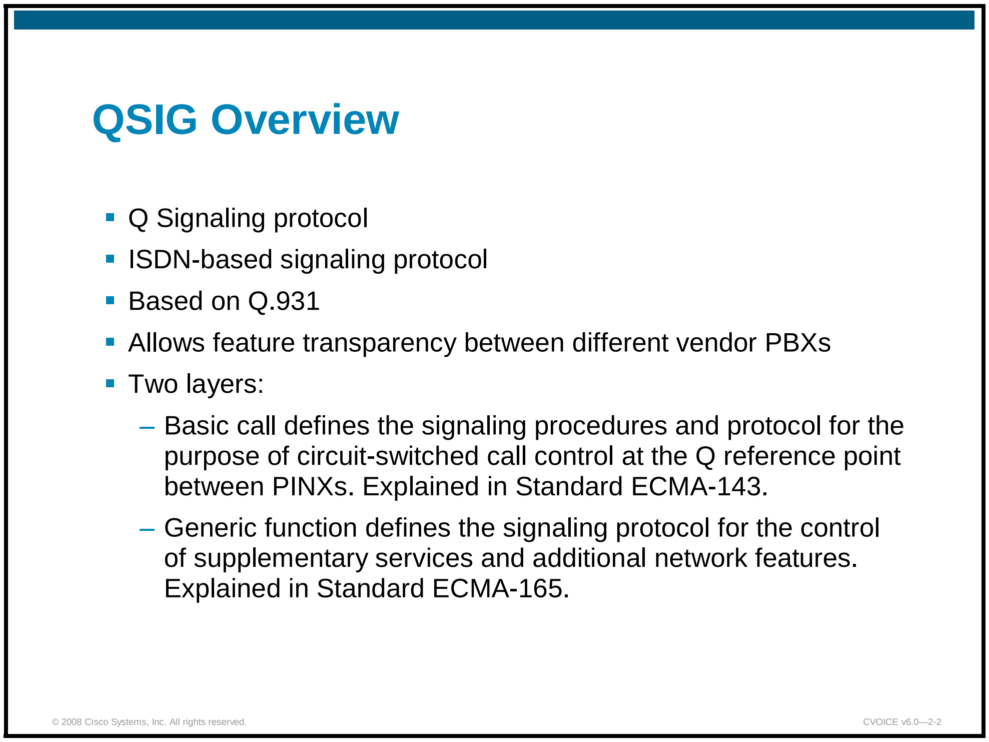
Objectives

Upon completing this lesson, you will be able to describe the key technologies that are used to implement ISDN QSIG trunks. This ability includes being able to meet these objectives:

- Describe QSIG and its associated features
- Describe how to configure QSIG support on Cisco IOS gateways
- Describe how to verify QSIG trunks

QSIG Overview

This topic describes the QSIG protocol and its associated features.



QSIG Overview

- Q Signaling protocol
- ISDN-based signaling protocol
- Based on Q.931
- Allows feature transparency between different vendor PBXs
- Two layers:
  - Basic call defines the signaling procedures and protocol for the purpose of circuit-switched call control at the Q reference point between PINXs. Explained in Standard ECMA-143.
  - Generic function defines the signaling protocol for the control of supplementary services and additional network features. Explained in Standard ECMA-165.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-2

QSIG is a variant of ISDN Q.921 and Q.931 ISDN data-channel (D-channel) signaling, for use in devices such as PBXs or key systems that are called Private Integrated services Network eXchange (PINX). Using QSIG signaling, a router can route incoming voice calls from a PINX across the WAN to a peer router, which can then transport the signaling and voice packets to another PINX. QSIG is becoming the standard for PBX interoperability in Europe and North America.

Cisco Unified Communications Manager nodes that support QSIG protocol or other equipment perform these functions:

- Telecommunications services within its own area
- Telecommunications services from the public ISDN or public switched telephone network (PSTN)
- Telecommunications services between PINXs in a multisite private network

QSIG ensures that the essential functions in Q.931 are carried from node to node

QSIG functions with these two sublayers:

- **QSIG basic call:** This standard defines the signaling procedures and protocol for the purpose of circuit-switched call control. This standard is based on Q.931.

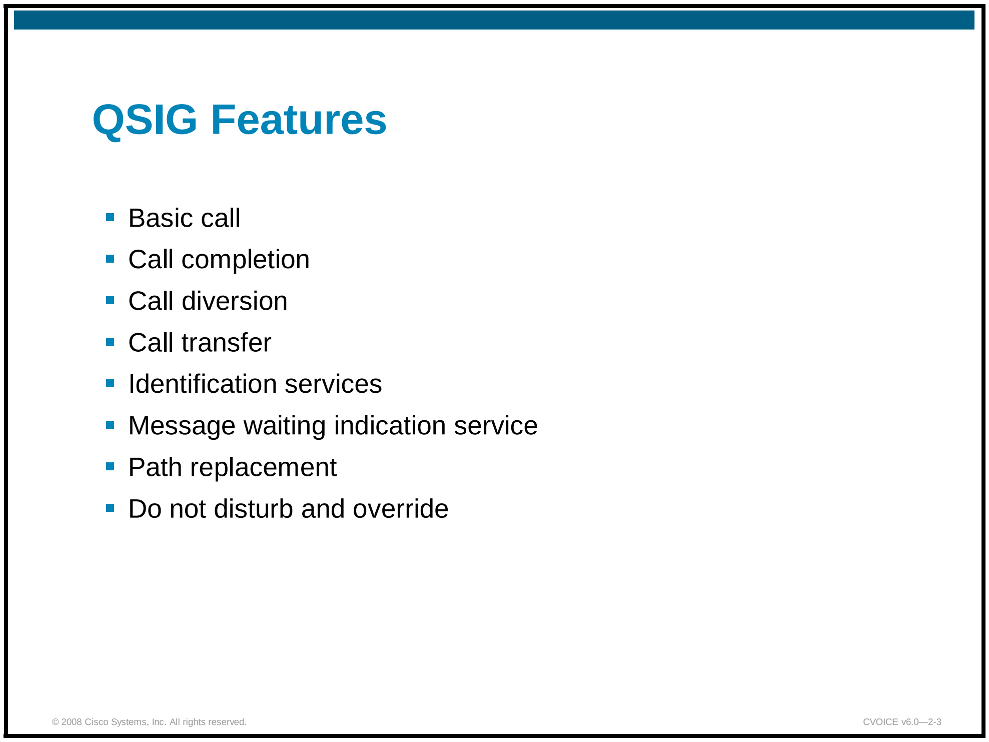
Note	See more QSIG basic call (Standard ECMA-143) information at http://www.ecma-international.org/publications/standards/Ecma-143.htm.

- **QSIG generic function:** This standard defines the signaling protocol for the control of supplementary services and additional network features at the Q reference point. This standard enables capabilities beyond basic call capability.

Note See more QSIG generic function (Standard ECMA-165) information at http://www.ecma-international.org/publications/standards/Ecma-165.htm.

QSIG Features

This subtopic covers QSIG features.



QSIG Features

- Basic call
- Call completion
- Call diversion
- Call transfer
- Identification services
- Message waiting indication service
- Path replacement
- Do not disturb and override

CVOICE v6.0—2-3

QSIG includes these features:

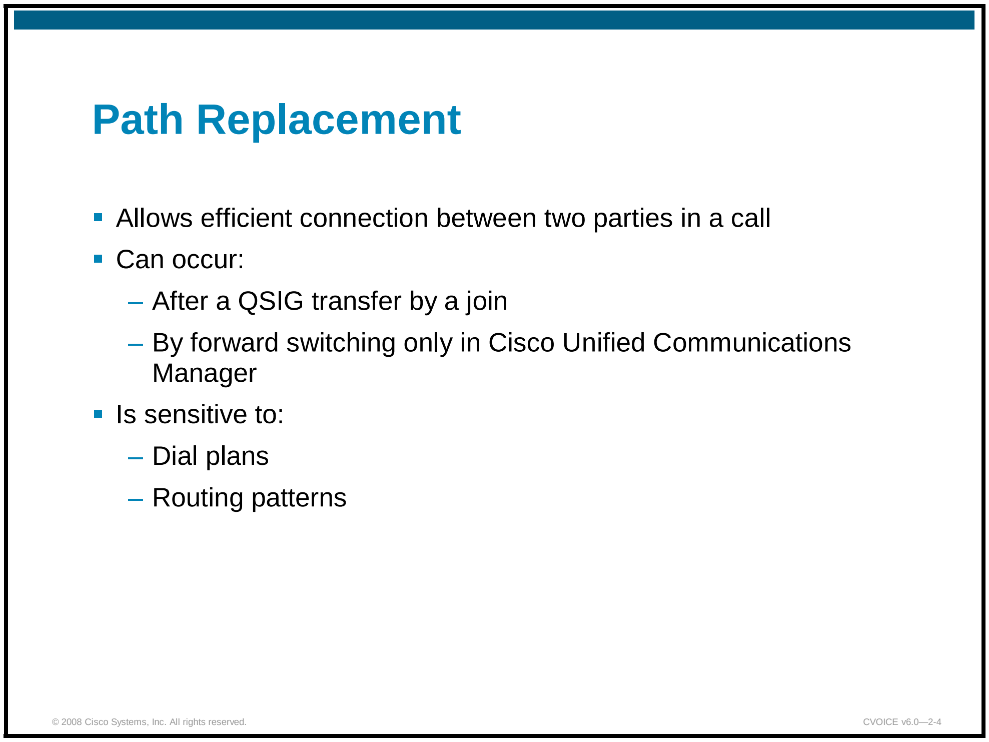
- **Basic call:** QSIG basic call setup provides the dynamic establishment of voice connections from an originating PINX (PBX or Cisco Unified Communications Manager) across a private network or virtual private network (VPN) to another PINX. You must use digital T1 or E1 PRI trunks to support QSIG protocol.
- **Call completion:** These call completion services rely on the facility selection and reservation feature and provide Cisco Call Back functionality over QSIG-enabled trunks:
  - **Completion of Calls to Busy Subscribers (CCBS):** When a calling party receives a busy tone, the caller can request that the call complete when the busy destination hangs up the phone and becomes available.
  - **Completion of Calls on No Reply (CCNR):** When a calling party receives no answer at the destination, the calling party can request that the call complete after the activity occurs on the phone of the called party.
- **Call diversion:** When call diversion by rerouting occurs, the originating PINX receives a request from the receiver of the call to divert the call to another user. The system creates a new call between the originator and the diverted-to user, and an additional Call Detail Record (CDR) gets generated. QSIG diversion supplementary services provide call-forwarding capabilities that are similar to familiar Cisco Unified Communications Manager call-forwarding features:
  - Call Forward All (CFA) configuration supports Call Forward Unconditional (CFU).
  - Call Forward Busy (CFB) configuration supports CFB.
  - Call Forward No Answer (CFNA) configuration supports Call Forwarding No Reply (CFNR).

To provide feature transparency with other PBXs in the network, the system passes information about a forwarded call during the call setup and connection over QSIG trunks. Phone displays can present calling name, number, or both; original called name, number, or both; and last redirecting name, number, or both to show the destination of the forwarded call.

- **Call transfer:** When a user transfers a call to another user, the QSIG identification service changes the connected name and number that displays on the transferred party phone. Call identification restrictions can impact what displays on the phone. The call transfer supplementary service interacts with the path replacement feature to optimize the trunk connections when a call transfers to a caller in another PINX.
- **Identification services:** When a call alerts and connects to a PINX, identification services can display the caller name, ID, or both on a phone in the terminating PINX, and likewise, the connected party name or ID on a phone in the originating PINX. QSIG identification restrictions enable you to control the presentation or display of this information between Cisco Unified Communications Manager and the connected PINX. Supported supplementary services apply on a per-call basis, and presentation settings for call identification information are set at both ends of the call.
- **Message waiting indication service:** In a QSIG network, when a PINX has a connected voice-messaging system that services users in another PINX, the PINX in the message center can send these MWI signals to the other PINX:
  - **MWI activate:** Sends a signal to activate MWI on the served user's phone after the voice-messaging system receives a message for that phone.
  - **MWI deactivate:** Sends a signal to deactivate the MWI after the user listens to messages in the associated voice-messaging system.
- **Do Not Disturb (DND) and Do Not Disturb Override (DNDO):** When a user does not want to be disturbed, the Private Integrated Services Network (PISN) can reject calls. DND and DNDO are described separately because DND is a service used by a called user, and DNDO is a service used by a calling user.
  - **DND:** Is a supplementary service that enables a user to cause the PISN to reject any calls, or just those associated with a specified basic service, addressed to the served user PISN number. The calling user is given an appropriate indication. Incoming calls are rejected as long as the service is active. The outgoing service of the served user is unaffected.
  - **DNDO:** Is a supplementary service that enables a user to override DND; that is, to allow the call to proceed as if the called user had not activated DND.

Path Replacement

This subtopic describes the ISDN path replacement feature.



Path Replacement

- Allows efficient connection between two parties in a call
- Can occur:
  - After a QSIG transfer by a join
  - By forward switching only in Cisco Unified Communications Manager
- Is sensitive to:
  - Dial plans
  - Routing patterns

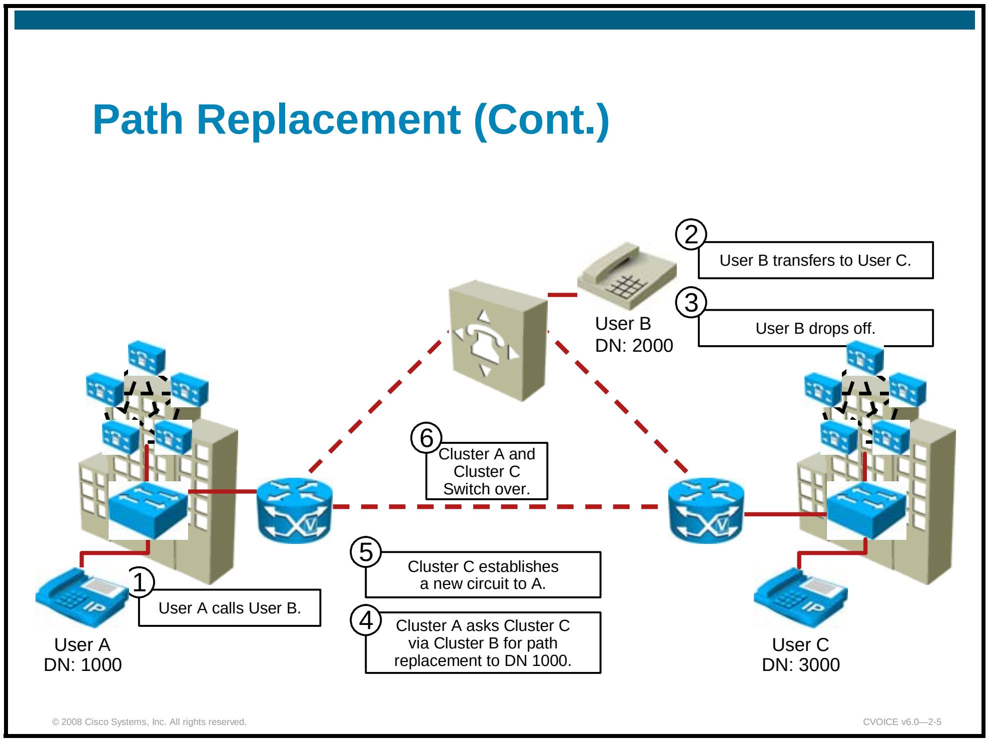
CVOICE v6.0—2-4

Path replacement allows for a potentially more efficient connection to be established between two parties in an active call. In Cisco Unified Communications Manager, this can occur after a QSIG transfer via a join or a diversion by forward switching.

In a QSIG network, after a call is transferred or forwarded to a phone in a third PINX, multiple connections through several PINXs can exist for the call. After the call connects, the path replacement feature drops the connection to the transit PINXs and creates a new call connection to the terminating PINX. Calls that involve multiple trunks (for example, conference calls) do not use path replacement. However, if you choose the QSIG option from the Tunneled Protocol drop-down list and check the Path Replacement Support check box for gatekeeper-controlled or non-gatekeeper-controlled intercluster trunks, path replacement occurs over the intercluster trunk and the other QSIG intercluster or PRI trunk that is used to transfer or divert the call.

It is important that you understand that the new path established by path replacement is not guaranteed to be more efficient—it is only “likely.” The network topology and route patterns in the network determine if and when the new path will be more optimal than the old path.

Path replacement does not get invoked by the Cisco Unified Communications Manager in other situations, such as a conference call.



Path Replacement (Cont.)

1 User A calls User B.

2 User B transfers to User C.

3 User B drops off.

4 Cluster A asks Cluster C via Cluster B for path replacement to DN 1000.

5 Cluster C establishes a new circuit to A.

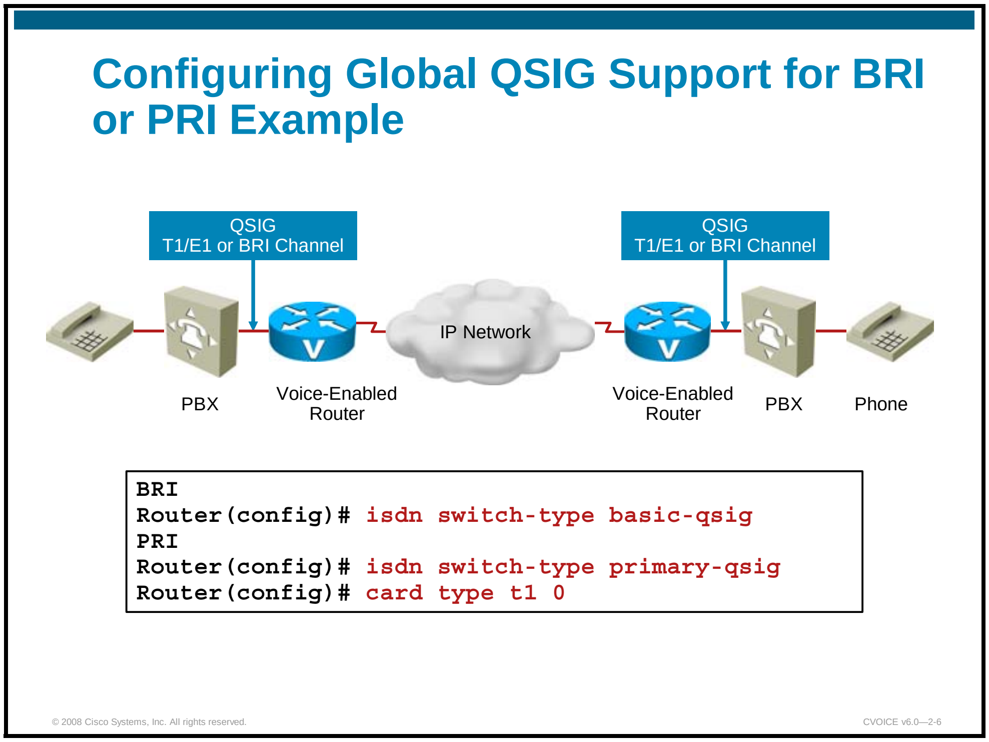
6 Cluster A and Cluster C Switch over.

Path replacement performs this procedure to replace the existing time-division multiplexing (TDM) circuits between two parties on an active call with new ones in order to use the TDM resources more efficiently:

1. User A calls User B.
2. User B transfers the call to user C.
3. User B drops off the call by pressing Transfer again.
4. Now Cluster A sends a message via B to C proposing that Cluster C should call directory number (DN) 1000 for a path replacement.
5. Cluster C establishes a new circuit to A.
6. Cluster C and Cluster A “switch over” the active call to use the new connection.

Configuring QSIG Support

This topic describes how to configure QSIG support on Cisco IOS gateways.



Configuring Global QSIG Support for BRI or PRI Example

```
BRI
Router(config)# isdn switch-type basic-qsig
PRI
Router(config)# isdn switch-type primary-qsig
Router(config)# card type t1 0
```

CVOICE v6.0—2-6

The diagram in the figure depicts a typical QSIG deployment topology.

Global QSIG Support Configuration Example

In this example, you have been tasked to configure a T1 controller for a voice gateway according to this network requirement:

- Connection type = PRI, using timeslots 1 to 24

Follow this procedure to configure global QSIG support for BRI or PRI.

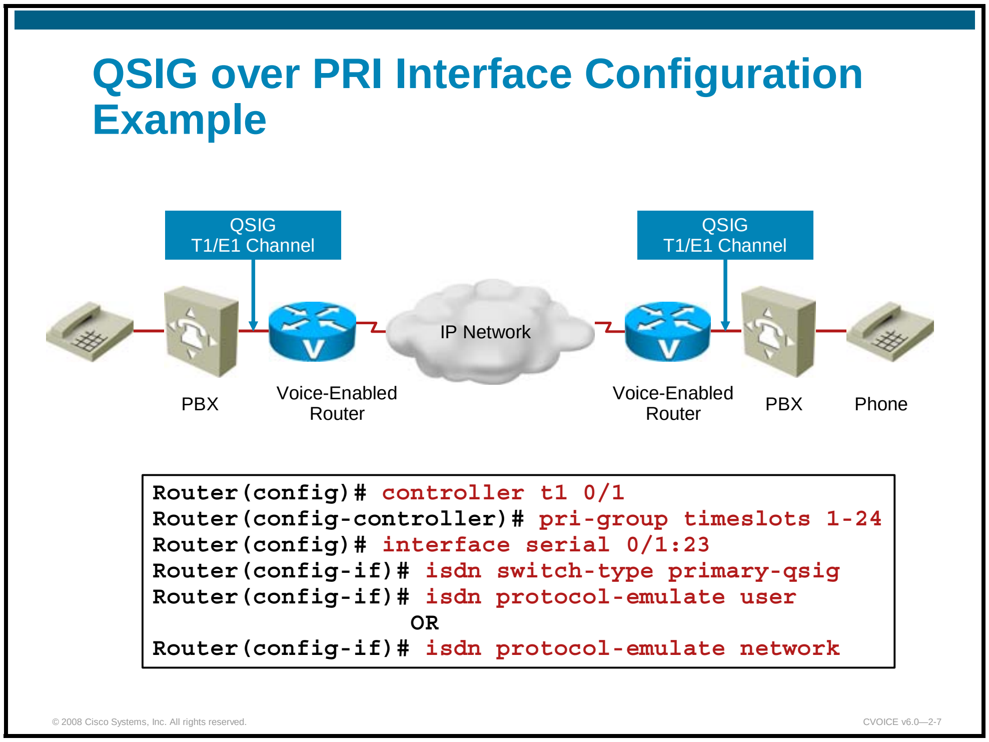
Step 1 Configure the global ISDN switch type to support QSIG signaling.

Step 2 Configure the digital signal processor (DSP) farm at the specified slot or port.

Step 3 Specify the card type (T1 or E1) at the specified slot so that the router provides sufficient DSP resources.

Configuring QSIG over PRI

This subtopic describes how to configure QSIG over PRI.



QSIG over PRI Interface Configuration Example

```
Router(config)# controller t1 0/1
Router(config-controller)# pri-group timeslots 1-24
Router(config)# interface serial 0/1:23
Router(config-if)# isdn switch-type primary-qsig
Router(config-if)# isdn protocol-emulate user
                  OR
Router(config-if)# isdn protocol-emulate network
```

CVOICE v6.0—2-7

The example in the figure shows a PRI QSIG support configuration.

Follow this procedure to configure the T1 or E1 controller for QSIG over PRI.

Step 1 Enter T1 or E1 controller configuration mode for the specified controller.

Step 2 Specify PRI on the timeslots that make up the PRI group. Separate low and high values with a hyphen.

- Maximum T1 range: 1-24
- Maximum E1 range: 1-31

Step 3 Enter interface configuration mode for the specified PRI slot/port and D-channel ISDN interface.

Note D-channel ISDN interface is (for T1) 23 and (for E1) 15.

Step 4 If you did configure the global PRI ISDN switch type for QSIG support in global configuration mode, this command overrides that command and configures the interface ISDN switch type to support QSIG signaling.

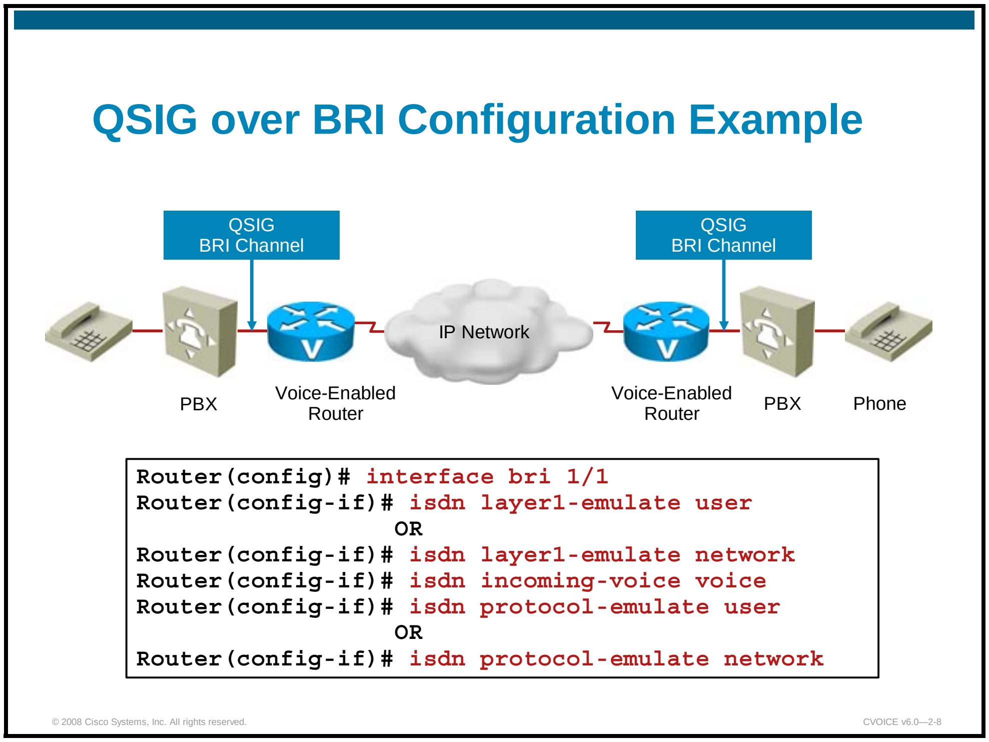
Step 4 (User side only) Configure Layer 2 and Layer 3 port mode emulation and clock status for the user, that is, the terminal equipment (clock slave). This is the default.

Or

(Network side only) Configure Layer 2 and Layer 3 port mode emulation and clock status for the network, that is, the Network Termination (NT) (clock master).

Configuring QSIG over BRI

This subtopic describes how to configure QSIG over BRI.



QSIG over BRI Configuration Example

```
Router(config)# interface bri 1/1
Router(config-if)# isdn layer1-emulate user
                   OR
Router(config-if)# isdn layer1-emulate network
Router(config-if)# isdn incoming-voice voice
Router(config-if)# isdn protocol-emulate user
                   OR
Router(config-if)# isdn protocol-emulate network
```

© 2008 Cisco Systems, Inc. All rights reserved.

CVOICE v6.0—2-8

Follow this procedure to configure QSIG support for BRI.

Step 1 Enter BRI configuration mode for the specified BRI.

Step 2 Configures Layer 1 port mode emulation and clock status for the user, that is, the terminal equipment (clock slave).

Step 3 Enable routing of incoming voice calls.

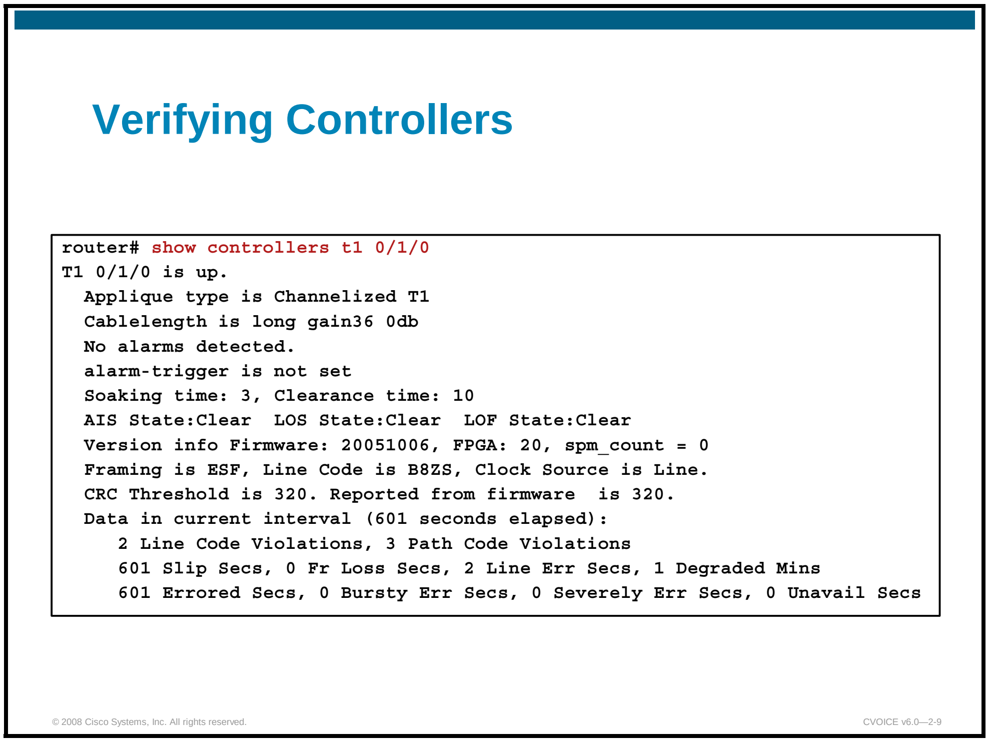
Step 4 (User side only) Configure Layer 2 and Layer 3 port mode emulation and clock status for the user, that is, the terminal equipment (clock slave).

Or

(Network side only) Configure Layer 2 and Layer 3 port mode emulation and clock status for the network, that is, the NT (clock master).

Verifying QSIG Trunks

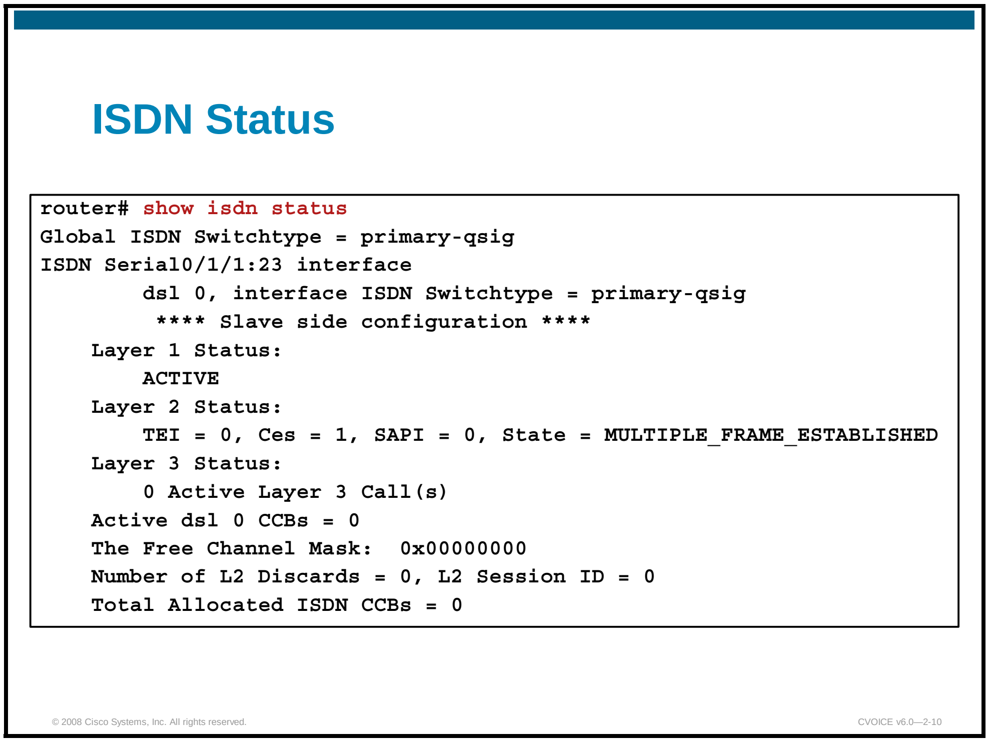
This topic describes how to verify QSIG trunks.



Verifying Controllers

```
router# show controllers t1 0/1/0
T1 0/1/0 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Version info Firmware: 20051006, FPGA: 20, spm_count = 0
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  CRC Threshold is 320. Reported from firmware  is 320.
  Data in current interval (601 seconds elapsed):
     2 Line Code Violations, 3 Path Code Violations
     601 Slip Secs, 0 Fr Loss Secs, 2 Line Err Secs, 1 Degraded Mins
     601 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

To display information about the PRI controller, use the **show controllers** command.

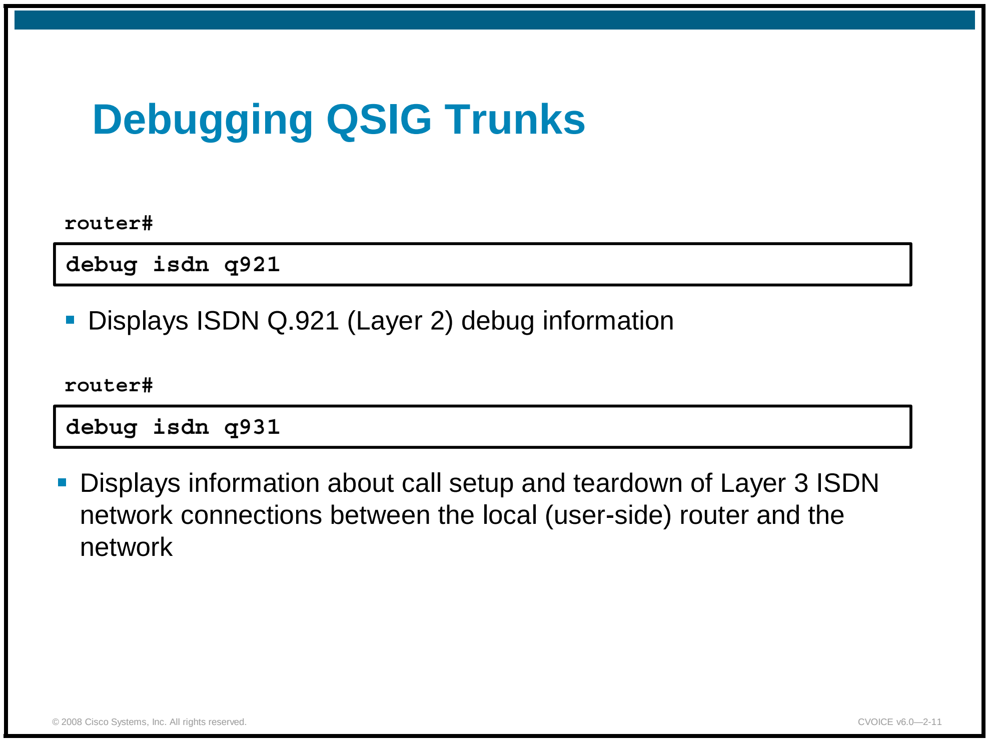


ISDN Status

```
router# show isdn status
Global ISDN Switchtype = primary-qsig
ISDN Serial0/1/1:23 interface
        dsl 0, interface ISDN Switchtype = primary-qsig
         **** Slave side configuration ****
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x00000000
    Number of L2 Discards = 0, L2 Session ID = 0
    Total Allocated ISDN CCBs = 0
```

Use the **show isdn status** command to verify that the ISDN Layer 1 is shown as ACTIVE and the Layer 2 state is MULTIPLE_FRAME_ESTABLISHED. If these conditions are satisfied, any problem that you encounter with the QSIG trunk is probably not with ISDN Layer 1 or Layer 2, and troubleshooting should focus on ISDN Layer 3 using the **debug isdn q931** command. If a TEI_UNASSIGNED or AWAITING_ESTABLISHMENT state is reported, verify the configuration. For a back-to-back configuration, such as in a connection between a voice gateway and a PBX, one of the sides must be set to emulate the network.

Note Remember, if network emulation is not correctly set, Layer 2 will not come up.



Debugging QSIG Trunks

```
router#
debug isdn q921
```

- Displays ISDN Q.921 (Layer 2) debug information

```
router#
debug isdn q931
```

- Displays information about call setup and teardown of Layer 3 ISDN network connections between the local (user-side) router and the network

© 2008 Cisco Systems, Inc. All rights reserved.   CVOICE v6.0—2-11

There are a few commands that you can use to debug a QSIG trunk.

debug isdn q921

The **debug isdn q921** command output is limited to commands and responses that are exchanged during peer-to-peer communication that is carried over the D channel. This debug information does not include data that is transmitted over the B channels that are also part of the router ISDN interface. The peers (data link layer entities and layer management entities on the routers) communicate with each other with an ISDN switch over the D channel.

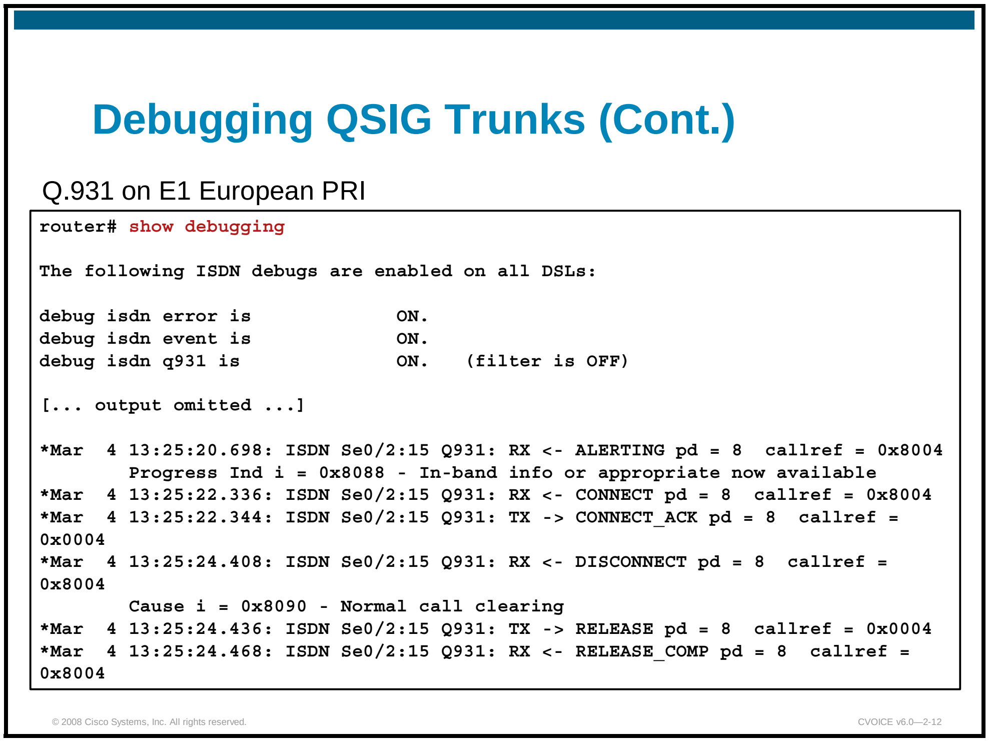
Note The ISDN switch provides the network interface that is defined by Q.921. This debug command does not display data link layer access procedures taking place within the ISDN network (that is, procedures taking place on the network side of the ISDN connection).

A router can be the calling or called party of the ISDN Q.921 data link layer access procedures. If the router is the calling party, the command displays information about an outgoing call. If the router is the called party, the command displays information about an incoming call and the keepalives.

You can use the **debug isdn q921** command simultaneously with the **debug isdn event**, **debug isdn q931**, **debug isdn q921 frame**, and **debug isdn q921 detail** commands. The displays are intermingled.

debug isdn q931

Use the **debug isdn q931** command to watch the Q.931 signaling messages go back and forth while the router negotiates the ISDN connection.



Debugging QSIG Trunks (Cont.)

Q.931 on E1 European PRI

```
router# show debugging

The following ISDN debugs are enabled on all DSLs:

debug isdn error is             ON.
debug isdn event is             ON.
debug isdn q931 is              ON.   (filter is OFF)

[... output omitted ...]

*Mar  4 13:25:20.698: ISDN Se0/2:15 Q931: RX <- ALERTING pd = 8  callref = 0x8004
        Progress Ind i = 0x8088 - In-band info or appropriate now available
*Mar  4 13:25:22.336: ISDN Se0/2:15 Q931: RX <- CONNECT pd = 8  callref = 0x8004
*Mar  4 13:25:22.344: ISDN Se0/2:15 Q931: TX -> CONNECT_ACK pd = 8  callref =
0x0004
*Mar  4 13:25:24.408: ISDN Se0/2:15 Q931: RX <- DISCONNECT pd = 8  callref =
0x8004
        Cause i = 0x8090 - Normal call clearing
*Mar  4 13:25:24.436: ISDN Se0/2:15 Q931: TX -> RELEASE pd = 8  callref = 0x0004
*Mar  4 13:25:24.468: ISDN Se0/2:15 Q931: RX <- RELEASE_COMP pd = 8  callref =
0x8004
```

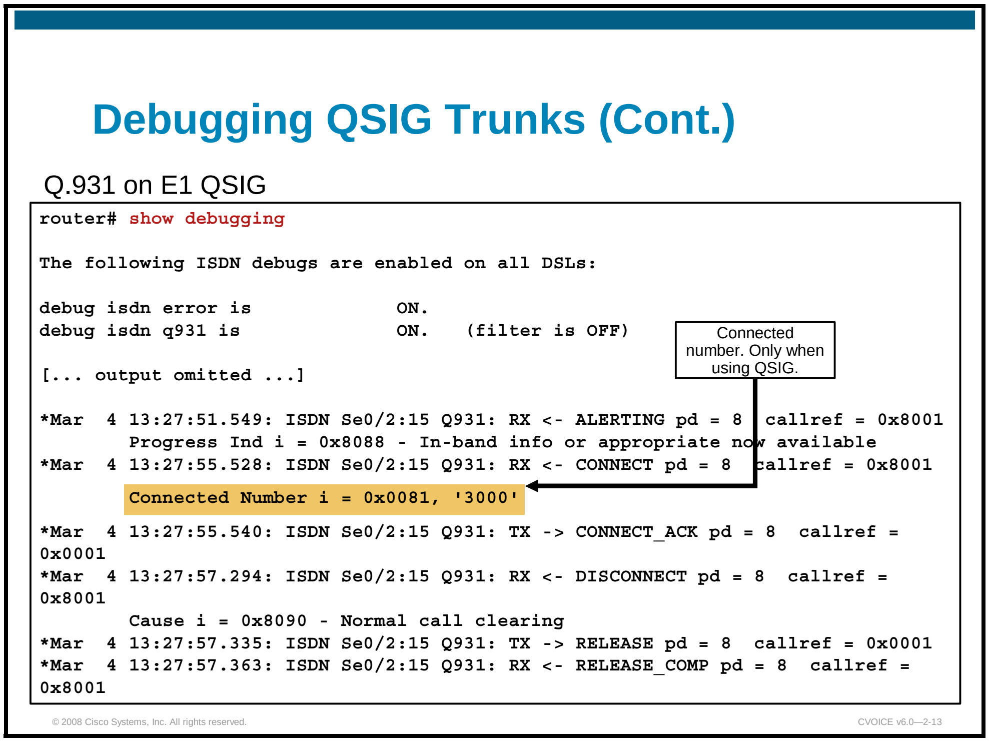
CVOICE v6.0—2-12

The output shows an ISDN Q.931 debug in an E1 European PRI environment.

Although the **debug isdn event** and the **debug isdn q931** commands provide similar debug information, the information is displayed in a different format. If you want to see the information in both formats, enable both commands at the same time. The displays will be intermingled.

The ISDN events that can be displayed are Q.931 events (call setup and teardown of ISDN network connections).

Use the **show dialer** command to retrieve information about the status and configuration of the ISDN interface on the router.



Debugging QSIG Trunks (Cont.)

Q.931 on E1 QSIG

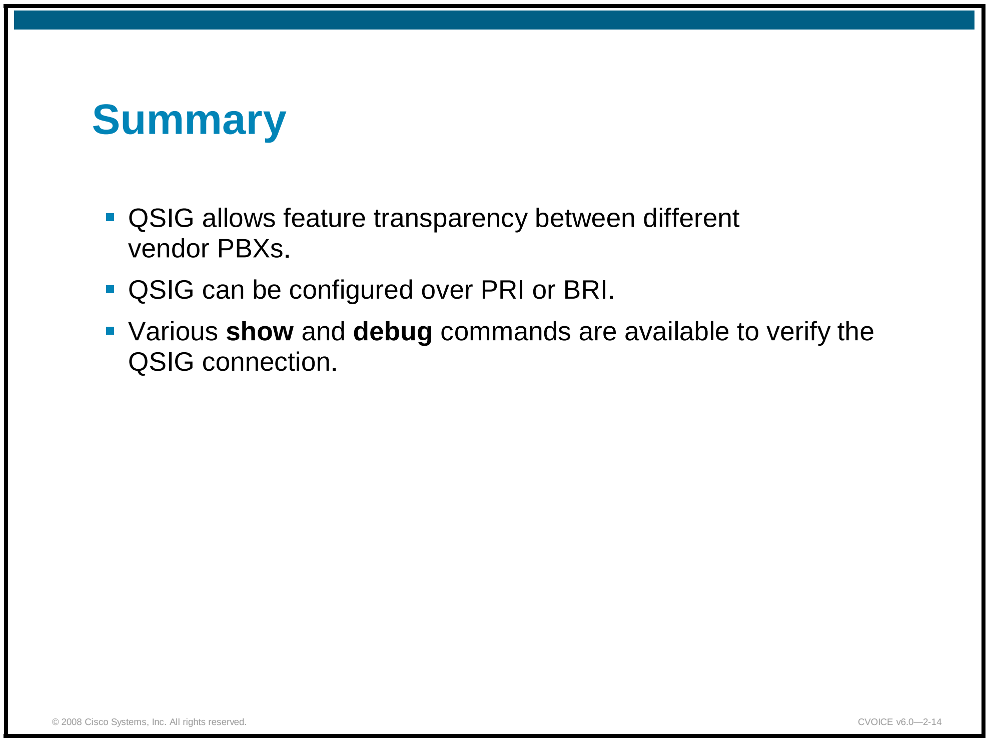
```
router# show debugging

The following ISDN debugs are enabled on all DSLs:

debug isdn error is              ON.
debug isdn q931 is               ON.   (filter is OFF)

[... output omitted ...]

*Mar  4 13:27:51.549: ISDN Se0/2:15 Q931: RX <- ALERTING pd = 8  callref = 0x8001
        Progress Ind i = 0x8088 - In-band info or appropriate now available
*Mar  4 13:27:55.528: ISDN Se0/2:15 Q931: RX <- CONNECT pd = 8  callref = 0x8001

        Connected Number i = 0x0081, '3000'

*Mar  4 13:27:55.540: ISDN Se0/2:15 Q931: TX -> CONNECT_ACK pd = 8  callref =
0x0001
*Mar  4 13:27:57.294: ISDN Se0/2:15 Q931: RX <- DISCONNECT pd = 8  callref =
0x8001
        Cause i = 0x8090 - Normal call clearing
*Mar  4 13:27:57.335: ISDN Se0/2:15 Q931: TX -> RELEASE pd = 8  callref = 0x0001
*Mar  4 13:27:57.363: ISDN Se0/2:15 Q931: RX <- RELEASE_COMP pd = 8  callref =
0x8001
```

Connected number. Only when using QSIG.

The output shows an ISDN Q.931 debug in an E1 QSIG environment. In contrast to the E1 European PRI, the QSIG connected number is available.

Summary

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



Summary

- QSIG allows feature transparency between different vendor PBXs.
- QSIG can be configured over PRI or BRI.
- Various **show** and **debug** commands are available to verify the QSIG connection.

CVOICE v6.0—2-14

Lesson Self-Check

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

Q1) Which two sublayers does QSIG use? (Choose two.)

Relates to: QSIG Overview

A) supplementary services
B) generic function
C) basic call
D) additional network features
E) advanced call setup

Q2) Which two are QSIG supplemental services or additional network features? (Choose two.)

Relates to: QSIG Overview

A) path replacement
B) do not disturb
C) identification conversion
D) address translation
E) path redirection

Q3) Which command specifies the ISDN switch type as PRI?

Relates to: Configuring QSIG Support

A) **isdn switch-type qsig-primary**
B) **isdn switch-type primary-qsig**
C) **isdn switch-type basic-qsig**
D) **isdn switch-type qsig-basic**

Q4) Which command specifies the ISDN switch type as BRI?

Relates to: Configuring QSIG Support

A) **isdn switch-type qsig-primary**
B) **isdn switch-type primary-qsig**
C) **isdn switch-type basic-qsig**
D) **isdn switch-type qsig-basic**

Q5) Which command would you use to verify that the ISDN switch type is set to **primary-qsig**.

Relates to: Verifying QSIG Trunks

A) **debug isdn events**
B) **debug isdn q931**
C) **show controllers**
D) **show isdn status**

Q6) Which command would you use to display information about the ISDN PRI?

Relates to: Verifying QSIG Trunks

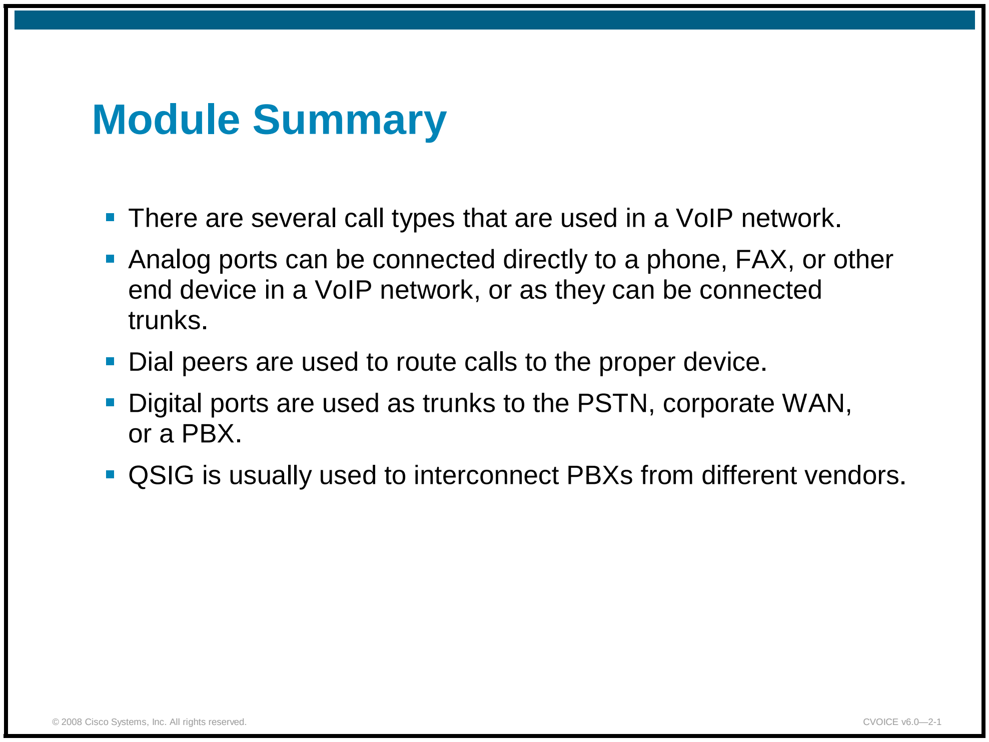
A) **debug isdn events**
B) **debug isdn q931**
C) **show controllers**
D) **show isdn status**

Lesson Self-Check Answer Key

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

Module Summary

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



Module Summary

- There are several call types that are used in a VoIP network.
- Analog ports can be connected directly to a phone, FAX, or other end device in a VoIP network, or as they can be connected trunks.
- Dial peers are used to route calls to the proper device.
- Digital ports are used as trunks to the PSTN, corporate WAN, or a PBX.
- QSIG is usually used to interconnect PBXs from different vendors.

© 2008 Cisco Systems, Inc. All rights reserved. CVOICE v6.0—2-1

Connecting and configuring devices to a VoIP network requires you to have intimate knowledge of the types of connections and their signaling characteristics. Once the devices in a VoIP network have been installed and configured properly, the gateways must know where to route the calls. This module introduced the various analog and digital voice ports that are available on a Cisco IOS voice gateway. Configuration of analog ports and digital trunks was discussed and examples were given. This module introduced plain old telephone service (POTS) and VoIP dial peers and the functions they provide in an IP telephony environment.

References

For additional information, refer to these resources:

- Cisco Systems, Inc. *Cisco IOS Voice Port Configuration Guide.* http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/vpcg/index.htm.
- Mallory, D., K. Salhoff, and D. Donohue. *Cisco Voice Gateways and Gatekeepers,* Cisco Press. August 2006.
- Cisco Systems, Inc. *Voice Network Signaling and Control.* http://www.cisco.com/en/US/customer/tech/tk652/tk653/technologies_tech_note09186a00800a6210.shtml#topic1.
- Cisco Systems, Inc. *Verifying Analog and Digital Voice-Port Configurations.* http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/vpcg/ch8_verf.htm.

- Cisco Systems, Inc. *Dial Peer Configuration on Voice Gateway Routers.* http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/index.htm.
- Cisco Systems, Inc. *Configuring Digital Voice Ports.* http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/vpcg/ch3_dgtl.htm.
- Cisco Systems, Inc. *Cisco IOS Debug Command Reference, Release 12.4T.* http://www.cisco.com/en/US/products/ps6441/products_command_reference_book09186a0080497a2b.html.
- Cisco Systems, Inc. *Cisco IOS ISDN Voice Configuration Guide.* http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/isdnv_c/index.htm.
- Ecma International. *Overview of Standards for Services and Signalling in Narrowband PISNs.* http://www.ecma-international.org/activities/Communications/N-PISN.htm.
- Cisco Systems, Inc. *Understanding Support for Voice and Data on 2600/3600 Series Routers.* http://www.cisco.com/en/US/products/hw/routers/ps259/products_tech_note09186a0080100688.shtml#fracpri.
- Tampa Bay Interactive, Inc. *ISDN D-Channel Operation.* http://telecom.tbi.net/isdn-d.htm.
- Protocols.com. ISDN Protocols. http://www.protocols.com/pbook/isdn.htm.