CCVP Learning

Authorized Self-Study Guide

Cisco Voice over IP (CVOICE)

Third Edition

Foundation learning for CVOICE exam 642-436

ciscopress.com

Kevin Wallace, CCIE® No. 7945

Authorized Self-Study Guide

Cisco Voice over IP (CVOICE), Third Edition

Kevin Wallace

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing July 2008

Library of Congress Cataloging-in-Publication Data:
Wallace, Kevin, CCNP.
Authorized self-study guide : Cisco Voice over IP (CVoice) / Kevin Wallace. — 3rd ed.
p. cm.
ISBN 978-1-58705-554-6 (hbk. : CD-ROM) 1. Internet telephony—Examinations—Study guides. 2. Electronic data processing personnel—Certification—Study guides. I. Title. II. Title: Cisco Voice over IP (CVoice).
TK5105.8865.W3345 2008
004.69'5—dc22
2008022672

ISBN-13: 978-1-58705-554-6

ISBN-10: 1-58705-554-6

Warning and Disclaimer

This book is designed to provide information about the Cisco Voice over IP (CVOICE) certification topics. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Foreword

Cisco certification Self-Study Guides are excellent self-study resources for networking professionals to maintain and increase internetworking skills and to prepare for Cisco Career Certification exams. Cisco Career Certifications are recognized worldwide and provide valuable, measurable rewards to networking professionals and their employers.

Cisco Press exam certification guides and preparation materials offer exceptional—and flexible—access to the knowledge and information required to stay current in one's field of expertise or to gain new skills. Whether used to increase internetworking skills or as a supplement to a formal certification preparation course, these materials offer networking professionals the information and knowledge required to perform on-the-job tasks proficiently.

Developed in conjunction with the Cisco certifications and training team, Cisco Press books are the only self-study books authorized by Cisco, and they offer students a series of exam practice tools and resource materials to help ensure that learners fully grasp the concepts and information presented.

Additional authorized Cisco instructor-led courses, e-learning, labs, and simulations are available exclusively from Cisco Learning Solutions Partners worldwide. To learn more, visit http://www.cisco.com/go/training.

I hope you will find this guide to be an essential part of your exam preparation and professional development, as well as a valuable addition to your personal library.

Drew Rosen

Manager, Learning & Development

Learning@Cisco

June 2008

Introduction

With the rapid adoption of Voice over IP (VoIP), many telephony and data network technicians, engineers, and designers are now working to become proficient in VoIP. Professional certifications, such as the Cisco Certified Voice Professional (CCVP) certification, offer validation of an employee's or a consultant's competency in specific technical areas.

This book mirrors the level of detail found in the Cisco CVOICE Version 6.0 course, which many CCVP candidates select as their first course in the CCVP track. Version 6.0 represents a significant update over Version 5.0 of the CVOICE course, because Version 6.0 integrates much of the content previously found in the more advanced Implementing Cisco Voice Gateways and Gatekeepers (GWGK) course.

A fundamental understanding of traditional telephony, however, would certainly benefit a CVOICE student or a reader of this book. If you think you lack a fundamental understanding of traditional telephony, a recommended companion for this book is the Cisco Press *Voice over IP First-Step* book (ISBN: 978-1-58720-156-1), which is also written by this book's author. *Voice over IP First-Step* is written in a conversational tone and teaches concepts surrounding traditional telephony and how those concepts translate into a VoIP environment.

Additional Study Resources

This book contains a CD with approximately 90 minutes of video, where you will see the author demonstrate a variety of basic VoIP configurations. The videos were originally developed for NetMaster Class (http://www.netmasterclass.com), a company specializing in CCIE Lab training. These video-on-demand titles are as follows:

Analog Voice Port Configuration

Digital Voice Port Configuration

Dial Peer Configuration

H.323 Configuration

MGCP Configuration

SIP Configuration

As an additional reference for readers pursuing the CCVP certification, the author has created a website with recommended study resources (some free and some recommended for purchase) for all courses in the CCVP track. These recommendations can be found at the following URL: http://www.voipcertprep.com.

Goals and Methods

The primary objective of this book is to help the reader pass the 642-436 CVOICE exam, which is a required exam for the CCVP certification and for the Cisco Rich Media Communications Specialist specialization.

One key methodology used in this book is to help you discover the exam topics that you need to review in more depth, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass by memorization, but helps you truly learn and understand the topics by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps, including detailed illustrations and topologies as well as sample configurations
- Providing exam practice questions to confirm your understanding of core concepts

Who Should Read This Book?

This book is primarily targeted toward candidates of the CVOICE exam. However, because CVOICE is one of the Cisco foundational VoIP courses, this book also serves as a VoIP primer to noncertification readers.

Many Cisco resellers actively encourage their employees to attain Cisco certifications and seek new employees already possessing Cisco certifications, for deeper discounts when purchasing Cisco products. Additionally, having attained a certification communicates to your employer or customer that you are serious about your craft and have not simply "hung out a shingle" declaring yourself knowledgeable about VoIP. Rather, you have proven your competency through a rigorous series of exams.

How This Book Is Organized

Although the chapters in this book could be read sequentially, the organization allows you to focus your reading on specific topics of interest. For example, if you already possess a strong VoIP background, you could skim the first two chapters (which cover foundational VoIP topics, including an introduction to VoIP and elements of a VoIP network) and focus on the remaining seven chapters, which address more advanced VoIP concepts. Specifically, the chapters in this book cover the following topics:

Chapter 1, "Introducing Voice over IP Networks": This chapter describes VoIP, components of a VoIP network, the protocols used, and service considerations of integrating VoIP into an existing data network. Also, this chapter considers various types of voice gateways and how to use gateways in different IP telephony environments.

Chapter 2, "Considering VoIP Design Elements": This chapter describes the challenges of integrating a voice and data network and explains solutions for avoiding problems when designing a VoIP network for optimal voice quality. Also, you learn the characteristics of voice codecs and digital signal processors and how to perform bandwidth calculations for VoIP calls.

Chapter 3, "Routing Calls over Analog Voice Ports": This chapter describes the various call types in a VoIP network. You then learn how to configure analog voice interfaces as new devices are introduced into the voice path. Finally, you discover how to configure dial peers, in order to add call routing intelligence to a router.

Chapter 4, "Performing Call Signaling over Digital Voice Ports": This chapter describes various digital interfaces and how to configure them. Also, you are introduced to Q Signaling (QSIG) and learn how to enable QSIG support.

Chapter 5, "Examining VoIP Gateways and Gateway Control Protocols": This chapter details the H.323, MGCP, and SIP protocol stacks, and you learn how to implement each of these protocols on Cisco IOS gateways.

Chapter 6, "Identifying Dial Plan Characteristics": This chapter describes the components and requirements of a dial plan and discusses how to implement a numbering plan using Cisco IOS gateways.

Chapter 7, "Configuring Advanced Dial Plans": This chapter shows you how to configure various digit manipulation strategies using Cisco IOS gateways. Additionally, you learn how to influence path selection. This chapter then concludes with a discussion of the Class of Restriction (COR) feature, and you learn how to implement COR on Cisco IOS gateways to specify calling privileges.

Chapter 8, "Configuring H.323 Gatekeepers": This chapter describes the function of a Cisco IOS gatekeeper. Also, you learn how to configure a gatekeeper for functions such as registration, address resolution, call routing, and call admission control (CAC).

Chapter 9, "Establishing a Connection with an Internet Telephony Service Provider": This chapter describes Cisco Unified Border Element (Cisco UBE) functions and features. You learn how a Cisco UBE is used in current enterprise environments and how to implement a Cisco UBE router to provide protocol interworking.

After reading this chapter, you should be able to perform the following tasks:

- Describe the various call types in a VoIP network.
- Configure analog voice interfaces as new devices are introduced into the voice path.
- Configure dial peers so you can add call routing intelligence to a router.

CHAPTER 3

Routing Calls over Analog Voice Ports

Voice gateways bridge the gap between the VoIP world and the traditional telephony world (for example, a private branch exchange [PBX], the public switched telephone network {PSTN], or an analog phone). Cisco voice gateways connect to traditional telephony devices via voice ports. This chapter introduces basic configuration of analog and digital voice ports and demonstrates how to fine-tune voice ports with port-specific configurations. Upon completing this chapter, you will be able to configure voice interfaces on Cisco voice-enabled equipment for connection to traditional, nonpacketized telephony equipment.

Introducing Analog Voice Applications on Cisco IOS Routers

Before delving into the specific syntax of configuring voice ports, this section considers several examples of voice applications. The applications discussed help illustrate the function of the voice ports, whose configuration is addressed in the next section.

Different types of applications require specific types of ports. In many instances, the type of port is dependent on the voice device connected to the network. Different types of voice applications include the following:

- Local calls
- On-net calls
- Off-net calls
- Private line, automatic ringdown (PLAR) calls
- PBX-to-PBX calls
- Intercluster trunk calls
- On-net to off-net calls

The following sections discuss each in detail and provide an example.

Local Calls

Local calls, as illustrated in Figure 3-1, occur between two telephones connected to one Cisco voice-enabled router. This type of call is handled entirely by the router and does not travel over an external network. Both telephones are directly connected to Foreign Exchange Station (FXS) ports on the router.

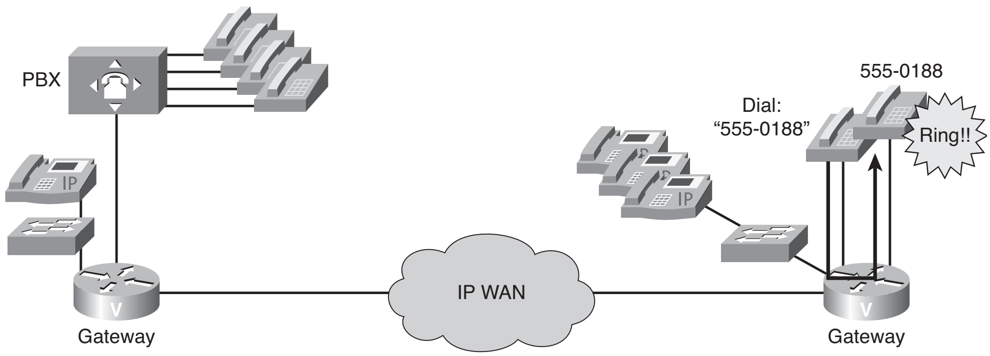

Figure 3-1 *Local Calls*

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

On-net calls occur between two telephones on the same data network, as shown in Figure 3-2. The calls can be routed through one or more Cisco voice-enabled routers, but the calls remain on the same data network. The edge telephones attach to the network through 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 through 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.

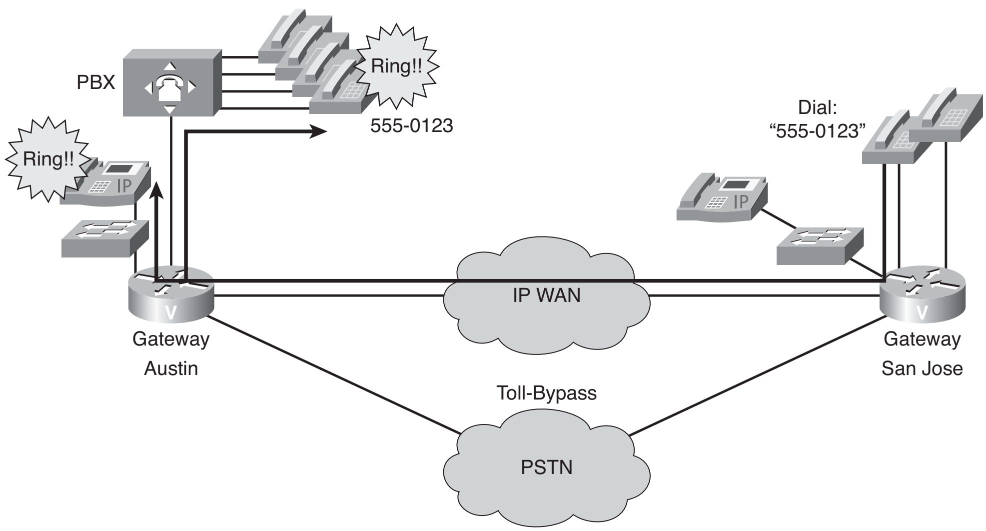

Figure 3-2 *On-Net Calls*

Note The act of routing voice data across the WAN instead of 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.

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 terminated on the remote office voice-enabled router.

Off-Net Calls

Figure 3-3 shows an example of an off-net call. To gain access to the PSTN, the user dials an access code, such as 9, from a telephone directly connected to a Cisco voice-enabled router or PBX. The connection to the PSTN is typically a single analog connection via a Foreign Exchange Office (FXO) port or a digital T1 or E1 connection.

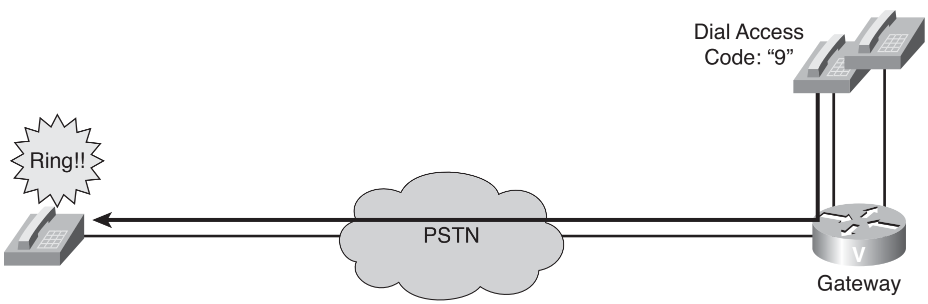

Figure 3-3 *Off-Net Calls*

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

PLAR calls automatically connect a telephone to a second telephone when the first telephone goes off hook, as depicted in Figure 3-4. When this connection occurs, the user does not get a dial tone, because the voice-enabled port that the telephone is connected to is preconfigured with a specific number to dial. A PLAR connection can work between any type of signaling, including E&M, FXO, FXS, or any combination of analog and digital interfaces. For example, you might have encountered a PLAR connection at an airline ticket counter where you pick up a handset and are immediately connected with an airline representative.

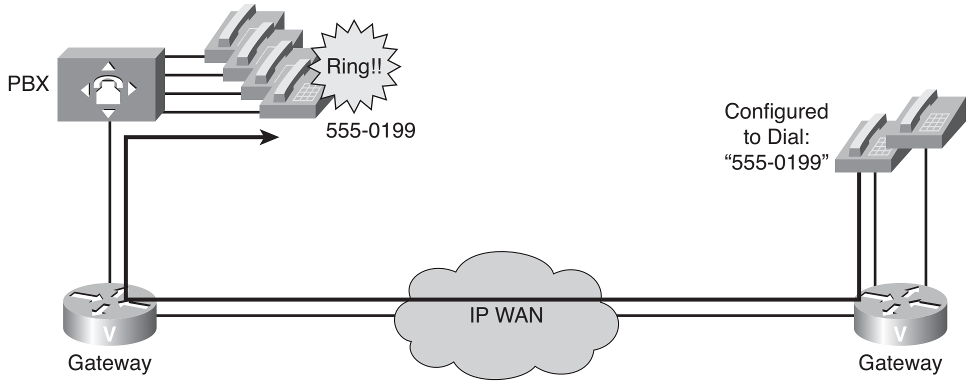

Figure 3-4 *PLAR Calls*

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

PBX-to-PBX calls, as shown in Figure 3-5, originate at a PBX at one site and terminate at a PBX at another site while using the network as the transport between the two locations. Many business environments connect sites with private tie trunks. When migrating to a converged voice and data network, this same tie-trunk connection can be emulated across an IP network. Modern PBX connections to a network are typically digital T1 or E1 with channel associated signaling (CAS) or Primary Rate Interface (PRI) signaling, although PBX connections can also be analog.

Note PBX-to-PBX calls are another form of toll-bypass.

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, through the remote voice-enabled router, and terminated on the remote office PBX.

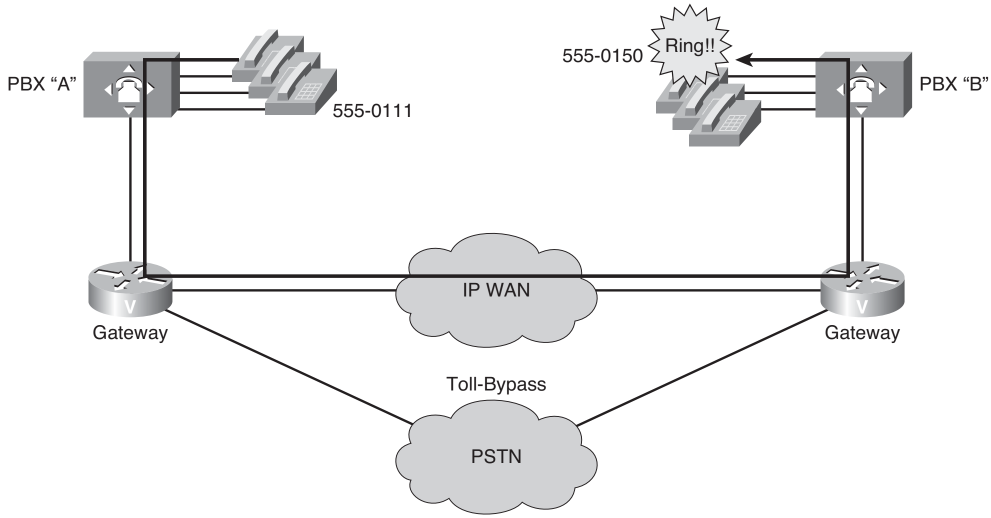

Figure 3-5 *PBX-to-PBX Calls*

Intercluster Trunk Calls

As part of an overall migration strategy, a business might replace PBXs with Cisco Unified Communications Managers. This includes IP phones connected to the IP network. Cisco Unified Communications Manager performs the call-routing functions 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 to a remote Cisco Unified Communications Manager for call completion. Intercluster trunk calls, as depicted in Figure 3-6, are routed between Cisco Unified Communications Manager clusters using a trunk.

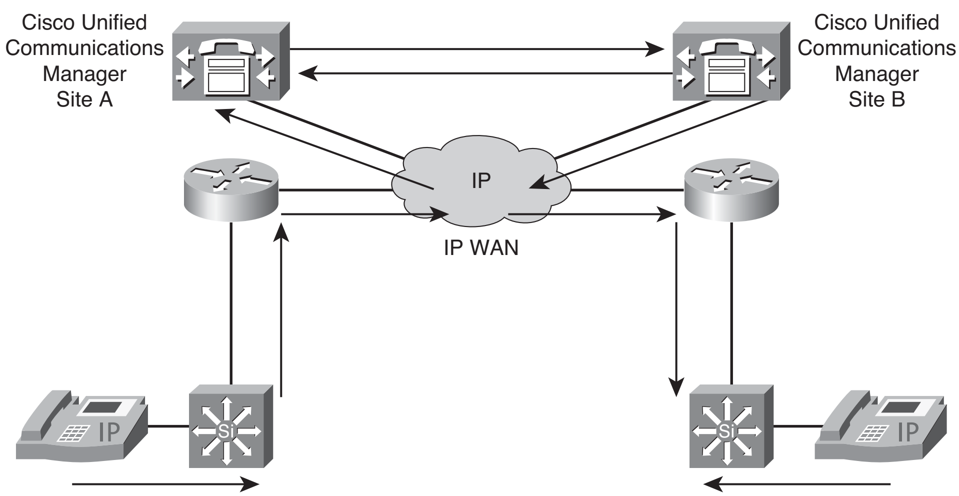

Figure 3-6 *Intercluster Trunk Calls*

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 Managers at each location. After the call is set up, the IP phones generate Real-time Transport Protocol (RTP) segments that carry voice data between sites.

On-Net to Off-Net Calls

When planning a resilient call-routing strategy, you might need to reroute calls through a secondary path should the primary path fail. An on-net to off-net call, as illustrated in Figure 3-7, originates on an internal network and is routed to an external network, usually to the PSTN. On-net to off-net call-switching functionality might be necessary when a network link is down or if a network becomes overloaded and unable to handle all calls presented.

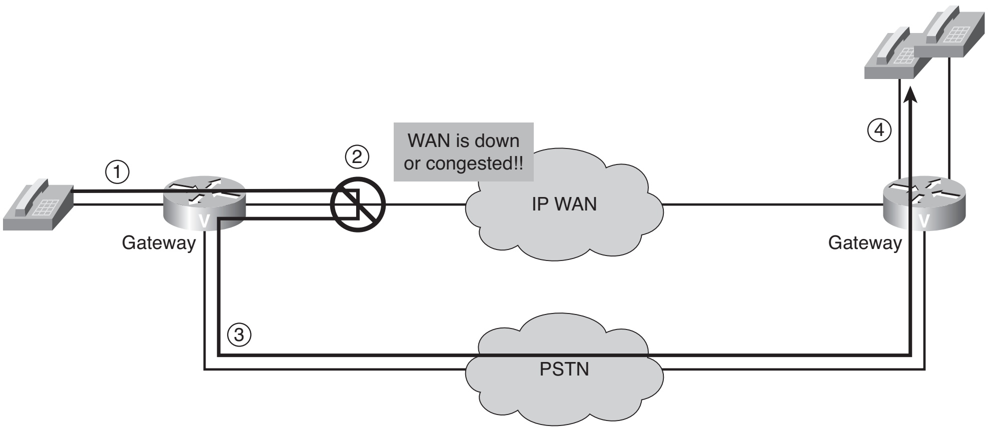

Figure 3-7 *On-Net to Off-Net Calls*

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

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 it cannot complete 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.

The following steps, numbered in Figure 3-7, summarize the call flow of an on-net to off-net call:

Step 1. A user on the network initiates a call to a remote site.

Step 2. The output of the WAN gateway is either down or congested, so the call is rerouted.

Step 3. The call connects to the PSTN.

Step 4. The PSTN completes the call to the remote site.

Summarizing Examples of Voice Port Applications

Table 3-1 lists application examples for each type of call.

Table 3-1 *Voice Port Call Types*

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

Introducing Analog Voice Ports on Cisco IOS Routers

Connecting voice devices to a network infrastructure requires an in-depth understanding of the signaling and electrical characteristics 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 section examines analog voice ports, analog signaling, and configuration parameters for analog voice ports.

Voice Ports

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 must be passed between the telephony devices at either end of the call, such as the on-hook status of the devices, the availability of the line, and whether an incoming call is trying to reach a device. 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 a circuit-switched network can understand. They must also be able to understand signaling information that is received from the circuit-switched network. This is accomplished by installing appropriate voice hardware in a router or access server and by configuring the voice ports that connect to telephony devices or the circuit-switched network. Figure 3-8 shows typical examples of how voice ports are used.

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.

These signaling interfaces generate information about things such as

- 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 they are interfacing with so calls can be exchanged smoothly between a packet network and a circuit-switched network.

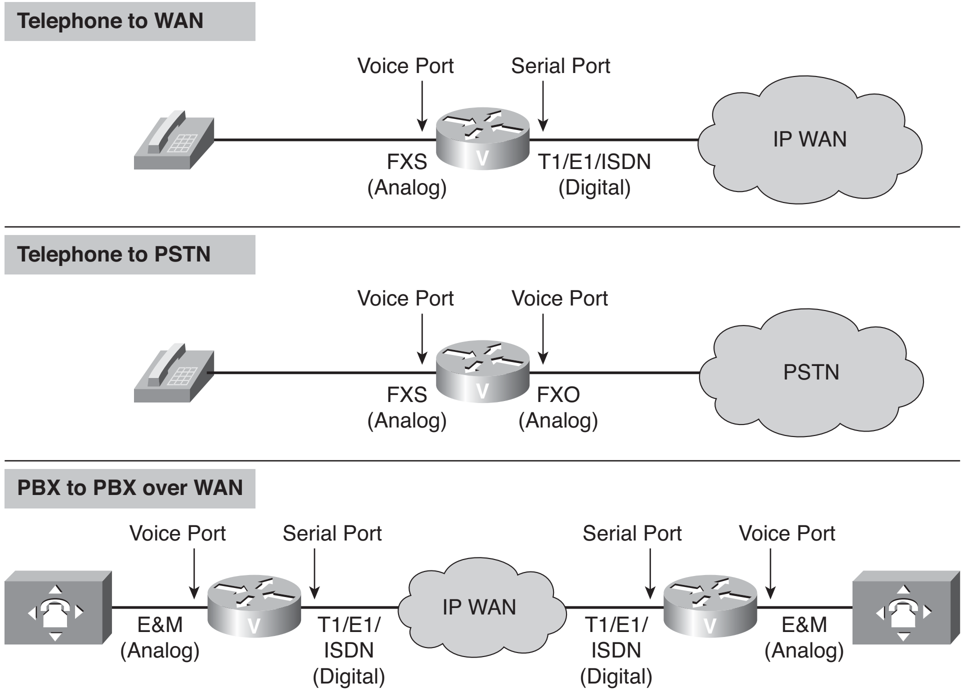

Figure 3-8 *Voice Ports*

The signaling interfaces discussed in the next sections include FXO, FXS, and 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

Analog voice port interfaces connect routers in packet-based networks to analog two-wire or four-wire 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. Three types of analog voice interfaces are supported by Cisco gateways, as illustrated in Figure 3-9.

The following is a detailed explanation of each of the three types of analog voice interfaces:

- **FXS:** 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.

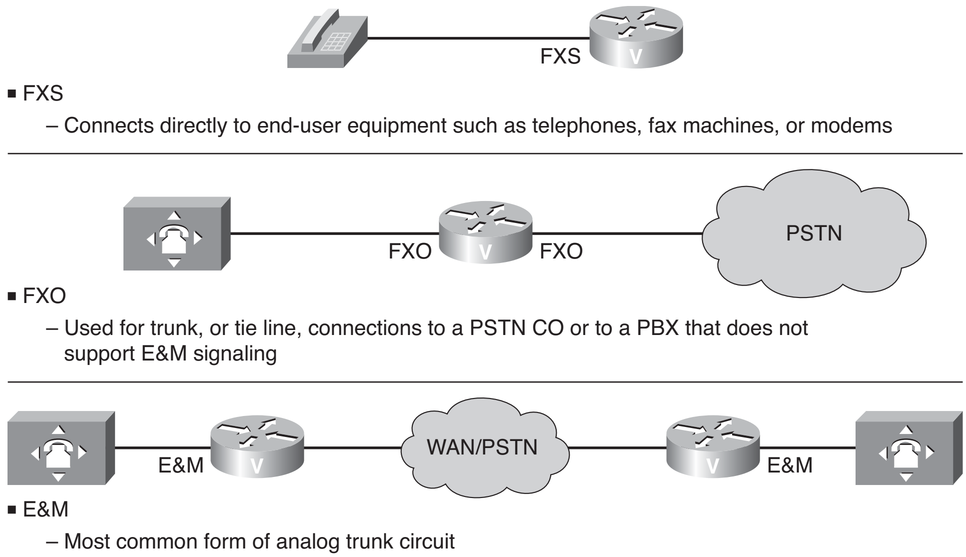

Figure 3-9 *Analog Voice Ports*

- **FXO:** 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 the 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:** 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 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 understanding and determine the direction of a signal in a wire.

  Like a serial port, an E&M interface has a DTE/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 might provide clocking 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

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 might 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. When 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 to the user, which indicates certain conditions such as an incoming call or a busy phone.

FXS and FXO Supervisory Signaling

FXS and FXO 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 telephone company's CO. Standard home telephone lines use loop-start, but business telephones can order ground-start lines instead.

Loop-Start

Loop-start, as shown in Figure 3-10, is the more common of the access signaling techniques. When a handset is picked up (the telephone goes off-hook), this action closes the 48V circuit that draws current from the telephone company CO and indicates a change in status, which signals the CO to provide a dial tone. An incoming call is signaled from the CO to the called handset by sending a signal in a standard on/off pattern, which causes the telephone to ring. When the called subscriber answers the call, the 48V circuit is closed and the CO turns off the ring voltage. At this point, the two circuits are tied together at the CO.

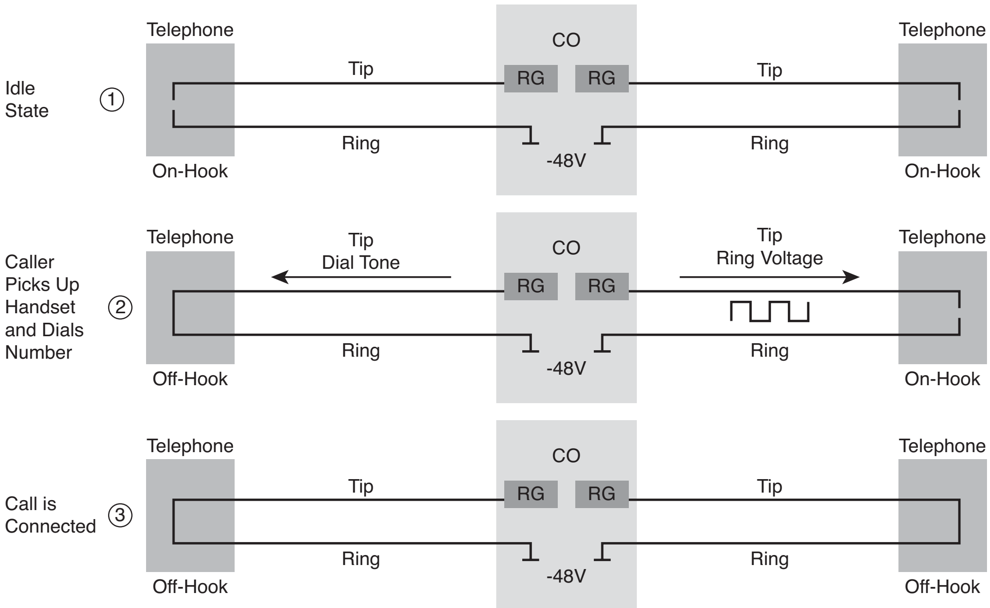

Figure 3-10 *Loop-Start Signaling*

The loop-start signaling process is as follows:

Step 1. In the idle state, the telephone, PBX, or FXO module has an open two-wire loop (tip and ring lines open). It could be a telephone set with the handset on-hook or a PBX or FXO module that generates an open between the tip and ring lines. The CO or FXS waits for a closed loop that generates a current flow. The CO or FXS have a ring generator connected to the tip line and −48VDC on the ring line.

Step 2. A telephone set, PBX, or FXO module closes the loop between the tip and ring lines. The telephone takes its handset 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. This indicates that the customer can start to dial. At the same time, the CO or FXS module seizes the ring line of the telephone, PBX, or FXO module called 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 after the telephone set, PBX, or FXO module closes the circuit between the tip and ring lines.

Step 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.

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 the glare problem because 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 ring-back tone.

Note 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 it receives through its FXO port. However, this function is not built in to the router for received calls. It operates only 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 experienced on business telephones.

Ground-Start

Ground-start signaling, as shown in Figure 3-11, 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.

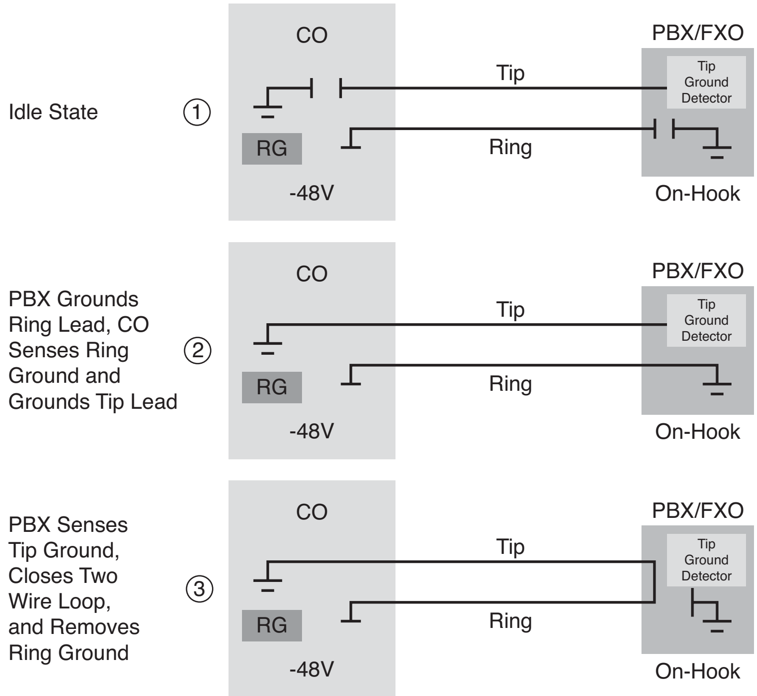

Figure 3-11 *Ground-Start Signaling*

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 and/or confirm switch 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.

The ground-start signaling process is as follows:

Step 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.

Step 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.

Step 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

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. Table 3-2 shows the frequency tones generated by dual tone multifrequency (DTMF) dialing.

Table 3-2 *DTMF Frequencies*

Frequencies	1209	1336	1477
697	1	2	3
770	4	5	6
852	7	8	9
941	*	0	#

Telephones use two different types of address signaling to notify the telephone company where a subscriber calls:

- 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 a call.

Pulsed tones were used by the old rotary phones. These phones had a disk that was 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.

These days, 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.

Informational Signaling

The FXS port provides informational signaling using *call progress* (CP) *tones*, as detailed in Table 3-3. These CP tones are audible and are used by the FXS connected device to indicate the status of calls.

Table 3-3 *Network Call Progress Tones*

Tone	Frequency (Hz)	On Time (sec)	Off Time (sec)
Dial	350 + 440	Continuous	Continuous
Busy	480 + 620	0.5	0.5
Ringback, line	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 to 400	Continuous	Continuous

The progress tones listed in Table 3-3 are for North American phone systems. International phone systems can have a totally different set of progress tones. Users should be familiar with most of the following call progress 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.
- **Ring-Back (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 processed.
- **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

E&M is another signaling technique used mainly between PBXs or other network-to-network telephony switches (Lucent 5 Electronic Switching System [5ESS], Nortel DMS-100, and so on). 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–V and Signaling System Direct Current No.5 (SSDC5). They use different methods to signal on-hook or off-hook status, as shown Table 3-4. Cisco voice implementation supports E&M Types I, II, III, and V.

Table 3-4 *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

The following list details the characteristics of each E&M signaling type introduced in Table 3-4:

- **Type I:** Type I signaling is the most common E&M signaling method used in North America. One wire is the E lead. The second wire is the M lead, and the remaining two pairs of wires serve as the audio path. In this arrangement, the PBX supplies power, or battery, for both E and M leads. In the idle (on-hook) state, both the E and M leads are open. 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 on Cisco voice gateways. However, Type IV operates similarly to Type II except for the M-lead operation. On Type IV, the M-lead states are open/ground, compared to Type II, which is open/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 leads are open as in the preceding diagram. The PBX indicates an off-hook by grounding the M lead. The line side indicates an off-hook by grounding the E lead.
- **SSDC5:** 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.

E&M 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 might 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 pairs of wires (four-wire).

E&M Address Signaling

PBXs built by different manufacturers can indicate on-hook/off-hook status and telephone line seizure on the E&M interface by using any of three types of access signaling:

- **Immediate-start:** Immediate-start, as illustrated in Figure 3-12, 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 signaling approach is used for E&M tie trunk interfaces.

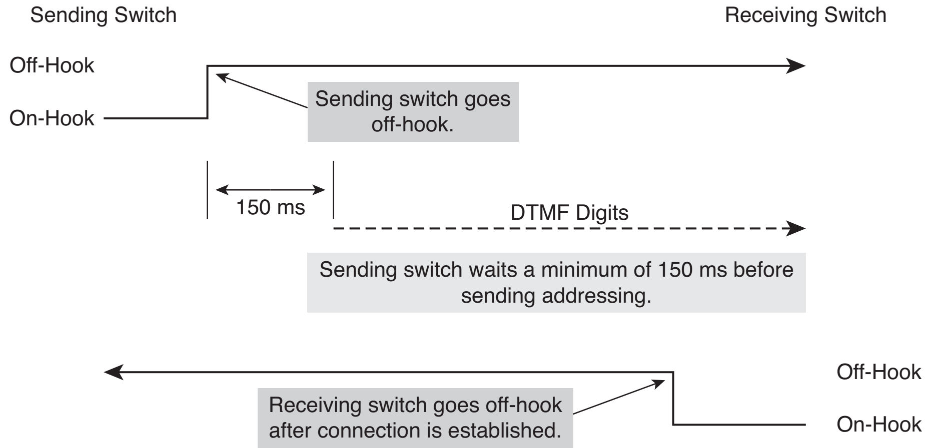

Figure 3-12 *Immediate-Start Signaling*

- **Wink-start:** Wink-start, as shown in Figure 3-13, is the most commonly used method for E&M access signaling and is 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; it 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 signaling is used for E&M tie trunk interfaces. This is the default setting for E&M voice ports.

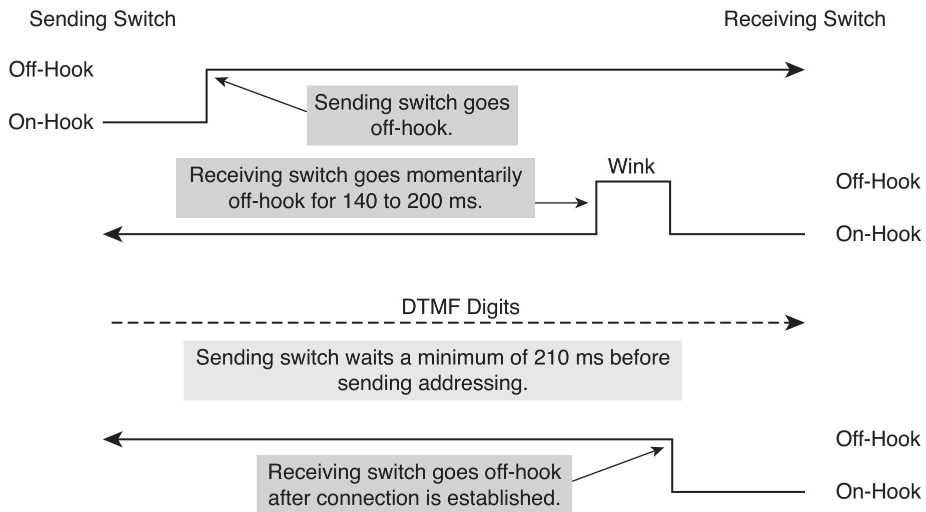

Figure 3-13 *Wink-Start Signaling*

- **Delay-start:** With delay-start signaling, as depicted in Figure 3-14, 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 signaling approach is used for E&M tie trunk interfaces.

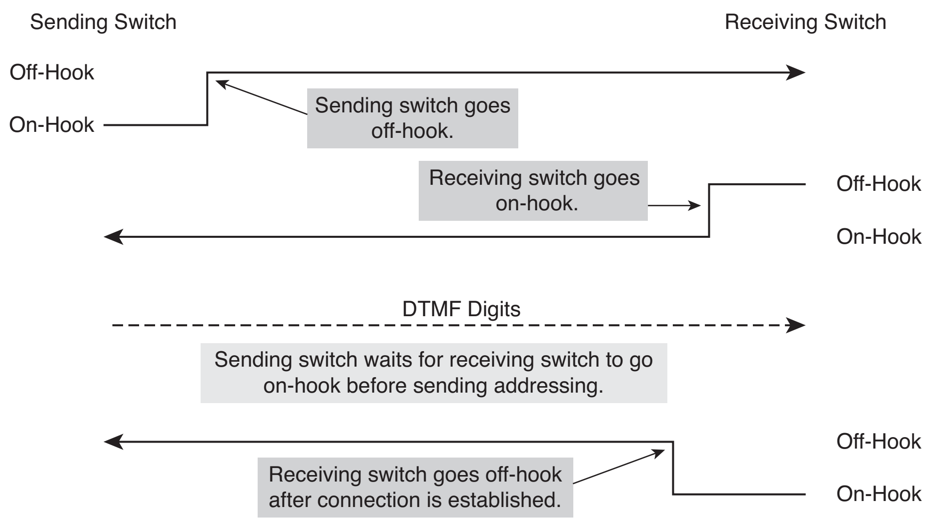

Figure 3-14 *Delay-Start Signaling*

Configuring Analog Voice Ports

The three types of analog ports that you will learn to configure are

- FXS
- FXO
- E&M

FXS Voice Port Configuration

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.

For example, consider an international company that 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.

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. Figure 3-15 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.

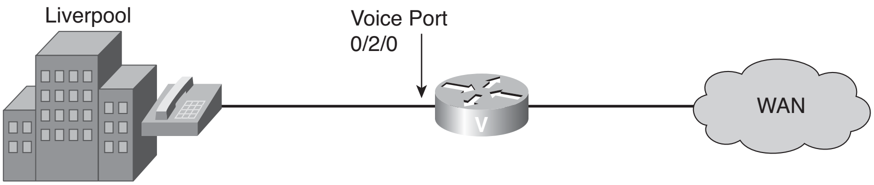

Figure 3-15 *FXS Configuration Topology*

The requirements for your configuration are the following:

- Configure the voice port to use ground-start signaling.
- Configure the call-progress tones for Great Britain.

You would then complete the following steps to accomplish the stated objectives:

Step 1. Enter voice-port configuration mode.

```
Router(config)#voice-port slot/port
```

Step 2. Select the access signaling type to match the telephony connection you are making.

```
Router(config-voiceport)#signal {loopstart | groundstart}
```

> **Note** If you change signal type, you must execute a **shutdown** and **no shutdown** command on the voice port.

Step 3. Select the two-letter locale for the voice call progress 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}
```

> **Note** The **patternXX** keyword provides preset ring-cadence patterns for use on any platform. The **define** keyword allows you to create a custom ring cadence.

Step 5. Activate the voice port.

```
Router(config-voiceport)#no shutdown
```

Example 3-1 shows the complete FXS voice port configuration.

Example 3-1 *FXS Voice Port Configuration*

```
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
```

FXO Voice Port Configuration

An FXO trunk is one of the simplest analog trunks available. Because Dialed Number Information Service (DNIS) information can only be sent out to the PSTN, no direct inward dialing (DID) is possible. ANI is supported for inbound calls. Two signaling types exist, loopstart and groundstart, with groundstart being the preferred method.

For example, consider the topology shown in Figure 3-16. Imagine you have been assigned to configure a voice gateway to route calls to and from the PSTN through an FXO port on the router.

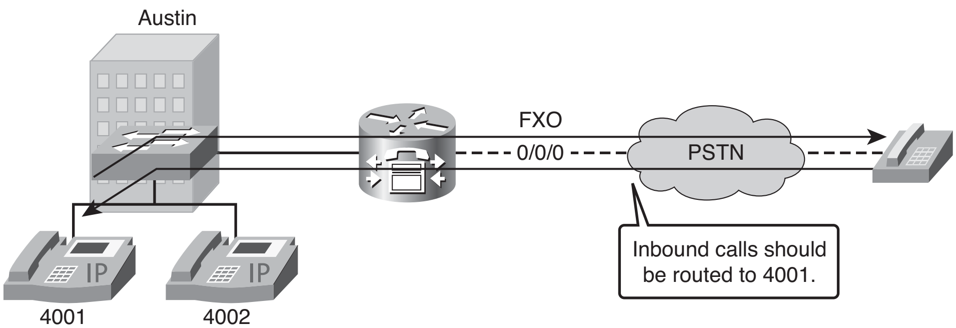

Figure 3-16 *FXO Configuration Topology*

In this scenario, you must set up a PLAR connection using an FXO port connected to the PSTN.

The configuration requirements are the following:

- 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.

You could then complete the following steps to configure the 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 the telephony connection 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
```

Note 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. This 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
```

Note 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.

Dial-peer configuration is covered in the section, "Introducing Dial Peers."

Step 8. Specify the voice port associated with this dial peer.

```
Router(config-dialpeer)#port 0/0/0
```

Example 3-2 shows the complete FXO voice port configuration.

Example 3-2 *FXO Voice Port Configuration*

```
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
```

E&M Voice Port Configuration

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

As an example, consider the topology shown in Figure 3-17.

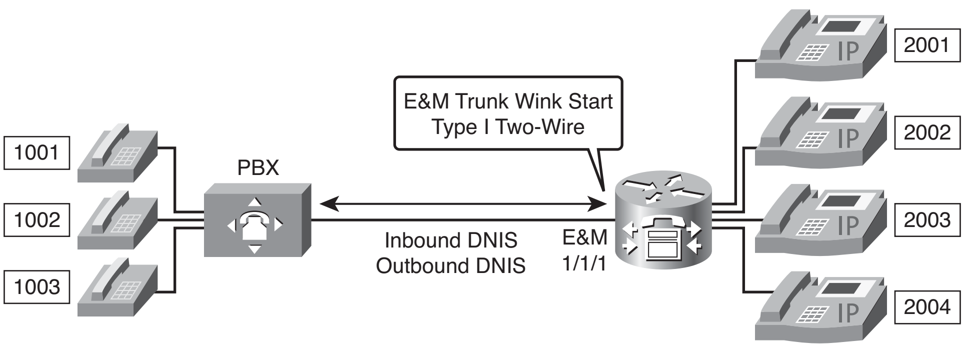

Figure 3-17 *E&M Configuration Topology*

In this example, you have been assigned to configure a voice gateway to work with an existing PBX system according to network requirements. 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 configuration requirements are the following:

- Configure the voice port to use wink-start signaling.
- Configure the voice port to use 2-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. The following 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 support is also configured on the corresponding dial peer.

You could then complete the following steps to configure the E&M voice port:

Step 1. Enter voice-port configuration mode.

Step 2. Select the access signaling type to match the telephony connection 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
```

Note This command affects only voice traffic. If the wrong cable scheme is specified, the user might get voice traffic in only one direction.

Also, 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 direct inward dial.

```
Router(config-dialpeer)#direct-inward-dial
```

Note DID is needed when POTS phones call IP Phones. In this case we match the POTS dial peer. This same dial peer is also used to call out to POTS phones.

Step 10. Specify digit forwarding all, so that no digits will be stripped as they are forwarded out of the voice port. By default, only digits matched by wildcard characters in the **destination-pattern** command are forwarded.

```
Router(config-dialpeer)#forward-digits all
```

Step 11. Specify the voice port associated with this dial peer.

```
Router(config-dialpeer)#port 1/1/1
```

Example 3-3 shows the complete E&M voice port configuration.

Example 3-3 *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
```

Trunks

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 could be a single FXO port that provides a single line connection between a Cisco gateway and a FXS port of small PBX system, a POTS device, or several T1 interfaces with 24 lines each in a Cisco gateway providing 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.

Figure 3-18 illustrates a variety of possible trunk connections.

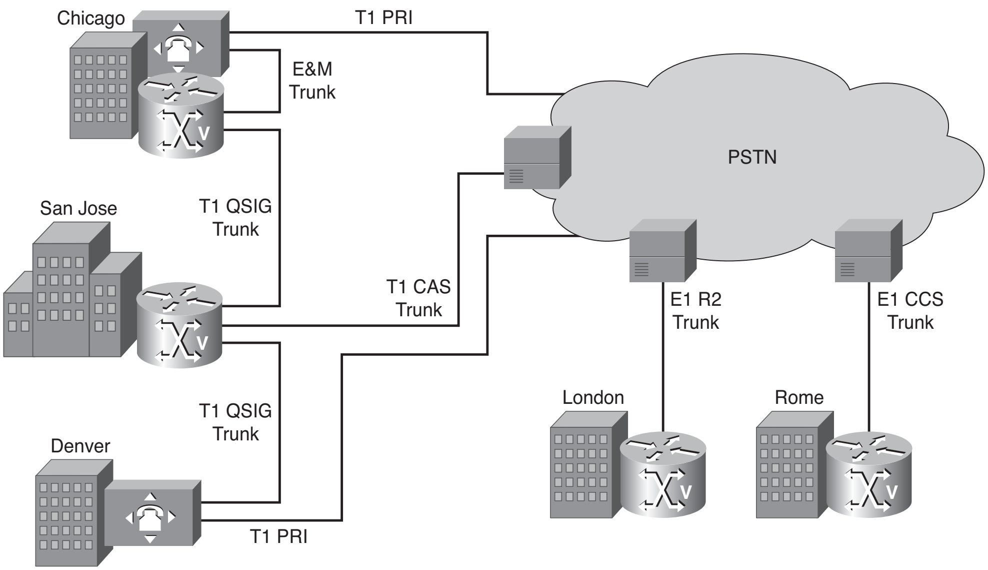

Figure 3-18 *E&M Trunks*

Consider the following characteristics of the trunks depicted in Figure 3-18:

- 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 connected to the Chicago gateway, the call will go via 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 Denver's Cisco IP telephony rollout has not started yet, the QSIG trunk is established directly between San Jose's gateway and Denver's legacy PBX.

Analog Trunks

Because many organizations continue to use analog devices, a requirement to integrate analog circuits with VoIP or IP telephony networks still exists. To implement a Cisco voice gateway into an analog trunk environment, the FXS, FXO, DID, and E&M interfaces are commonly used, as illustrated in Figure 3-19.

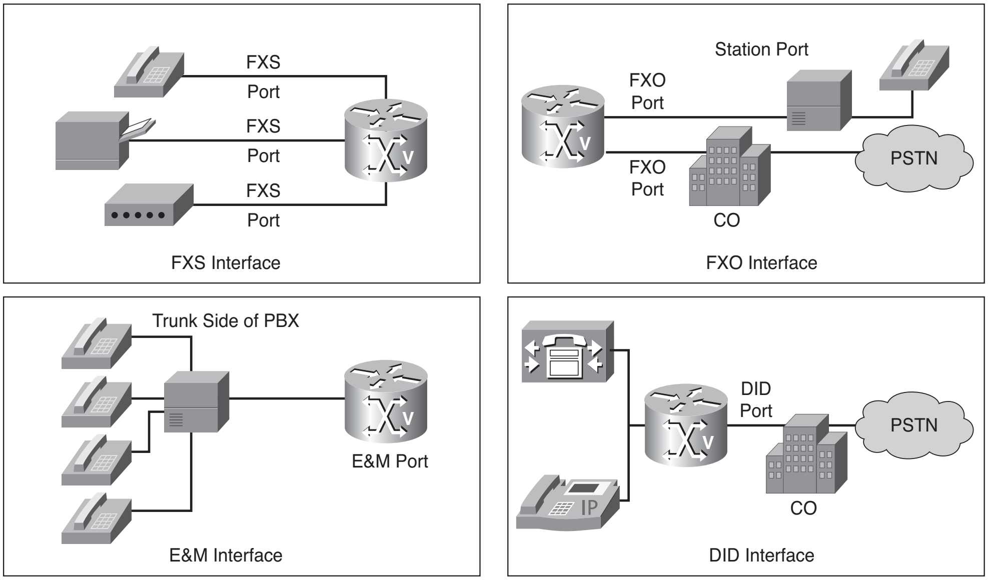

Figure 3-19 *Analog Trunks*

PSTN carriers typically offer analog trunk features that can be supported on home phones. Table 3-5 presents a description of the common analog trunk features.

Table 3-5 *Analog Trunk Features*

Feature	Description
Caller ID	Caller ID allows users to see the calling number before answering the phone.
Message waiting	Two methods activate an analog message indicator: ■ 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, the user 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.

Table 3-5 *Analog Trunk Features (continued)*

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.

Figure 3-20 shows small business voice networks 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.

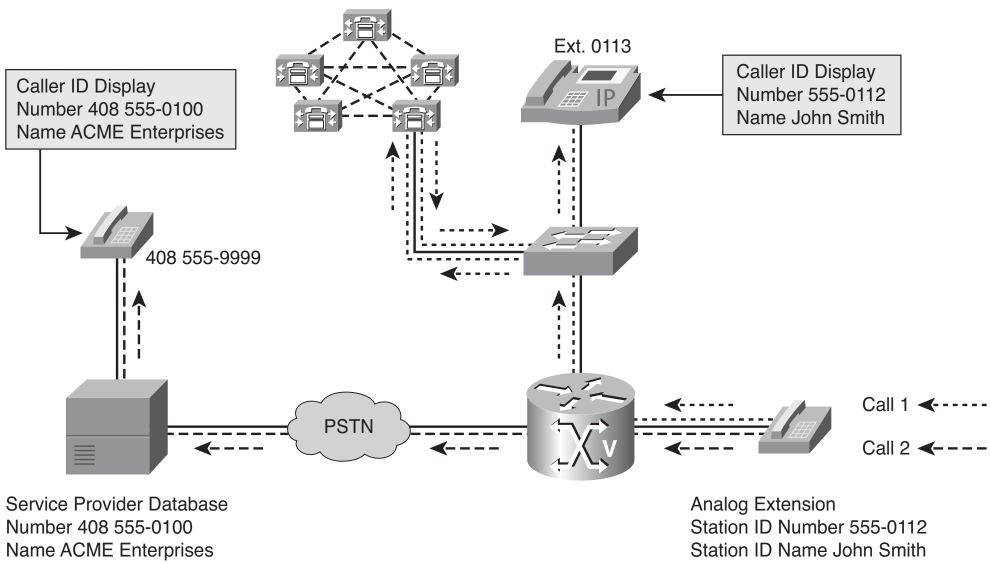

Figure 3-20 *Analog Trunks - Example*

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 555-0212. When a call is placed from the analog phone to another phone on the premises, an IP phone in this case, the caller name and number are displayed on the screen of the IP phone.
- **Call 2:** Call 2 is placed from the same analog phone, but the destination is off the premises on the PSTN. The FXO port forwards 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 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).

Centralized Automated Message Accounting

A Centralized Automated Message Accounting (CAMA) trunk is a special analog trunk type originally developed for long-distance billing but now mainly used for emergency call services (911 and E911 services). You can use CAMA ports to connect to a Public Safety Answering Point (PSAP) for emergency calls. A CAMA trunk can send only outbound automatic number identification (ANI) information, which is required by the local public safety answering point (PSAP).

CAMA interface cards and software configurations are targeted at corporate enterprise networks and at service providers and carriers who are creating new or supplementing existing networks with Enhanced 911 (E911) services. CAMA carries both calling and called numbers by using in-band signaling. This method of carrying identifying information 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 might 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.

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 ISRs. It is common for E911 service providers to require CAMA interfaces to their network.

Figure 3-21 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.

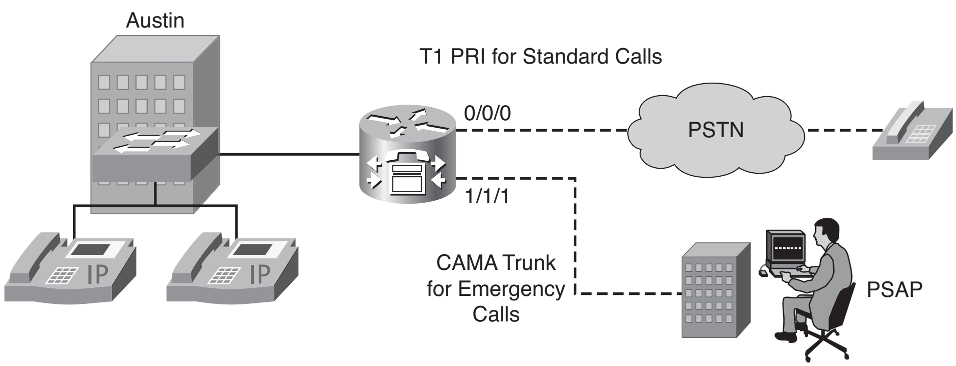

Figure 3-21 *Configuring a CAMA Trunk*

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. Five 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/Pseudo ANI (PANI).
- **KP-2-ST:** Default transmission when the CAMA trunk cannot get a corresponding Numbering Plan Digit (NPD) in the look-up table or when the calling number is fewer than 10 digits. (NPA digits are not available.)
- **KP-NPD-NXX-XXXX-ST**: 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, 3=916

  05551234 = (415) 555-1234, 15551234 = (510) 555-1234

  The NPD value range is 0–3.

When you use the NPD format, the area code needs to be associated with a single digit. You can preprogram the NPA into a single MF digit using the **ani mapping** voice port command. The number of NPDs programmed is determined by local policy as well as by the number of NPAs 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.

You could then complete the following steps to configure the voice port for CAMA operation:

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
```

Example 3-4 shows the complete CAMA trunk configuration.

Example 3-4 *CAMA Trunk Configuration*

```
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
```

Direct Inward Dial

Typically, FXS ports connect to analog phones, but some carriers offer FXS trunks that 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 555-1000 to 555-1999. A caller dials 555-1234, and the local CO forwards 234 to the PBX or VoIP system. The PBX or VoIP system then rings extension 234. This entire process is transparent to the caller.

An FXS DID trunk can receive only inbound calls, thus a combination of FXS, DID, and FXO ports is required for inbound and outbound calls. Two signaling types exist, loopstart and groundstart, with groundstart being the preferred method.

Figure 3-22 shows an analog trunk using an FXS DID trunk for inbound calls and a standard FXO trunk for outbound calls.

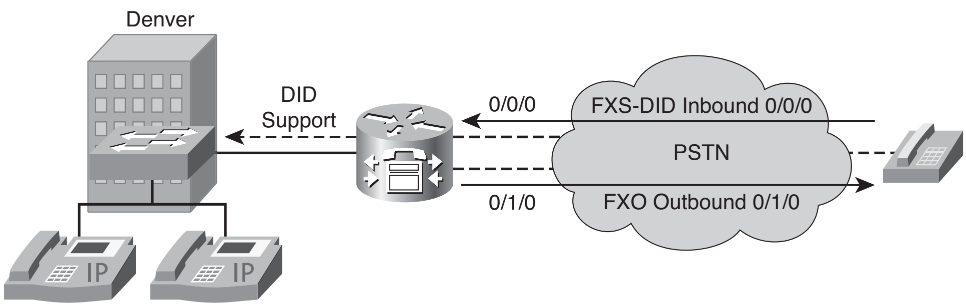

Figure 3-22 *Configuring DID Trunks*

You could then complete the following steps to enable DID signaling on the 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 groundstart 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 dial 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
```

Example 3-5 shows the complete DID trunk configuration.

Example 3-5 *DID Trunk Configuration*

```
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
```

Timers and Timing

You can set a number of timers and timing parameters for fine-tuning a voice port. Following are voice-port configuration mode commands you can use to a set variety of timing parameters:

- **timeouts initial** *seconds*: 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** *seconds*: Configures the number of seconds for which the system will wait between caller-entered digits before sending the input to be assessed. If the digits are coming from an automated device, and the dial plan is a variable-length dial plan, you can shorten this timer so the call proceeds without having to wait the full default of 10 seconds for the interdigit timer to expire.
- **timeouts ringing** {*seconds* | **infinity**}: Configures the length of time a caller can 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 a voice port when it is evident the call is not going to be answered.
- **timing digit** *milliseconds*: 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 might have trouble recognizing dialed digits. If a user or device dials too quickly, the digit might not be recognized. By changing the timing on the digit timer, you can provide for a shorter or longer DTMF duration.
- **timing interdigit** *milliseconds*: Configures the DTMF interdigit duration for a specified voice port. You can change this setting to accommodate faster or slower dialing characteristics.

- **timing hookflash-input** *milliseconds* and **hookflash-output** *milliseconds*: Configures the maximum duration (in milliseconds) of a hookflash indication. Hookflash is an indication by a caller that wants to do something specific with the call, such as transfer the call or place the call on hold. For the **hookflash-input** 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 might 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-output** 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. In two instances, 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

Example 3-6 shows a configuration for a home for someone with a disability that might require more time to dial digits. Notice the requirement to allow the telephone to ring, unanswered, for 4 minutes. The configuration 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** is set to 500 ms.

Example 3-6 *Timers and Timing Configuration*

```
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
```

Verifying Voice Ports

After physically connecting analog or digital devices to a Cisco voice-enabled router, you might need to issue **show**, **test**, or **debug** commands to verify or troubleshoot your configuration. For example, the following list enumerates six steps to monitor and troubleshoot voice ports:

Step 1. Pick up the handset of an attached telephony device and check for a dial tone. If there is no dial tone, check the following:

- Is the plug firmly seated?
- Is the voice port enabled?

- Is the voice port recognized by the Cisco IOS?
- Is the router running the correct version of Cisco IOS in order to recognize the module?
- Is a dial peer configured for that port?

Step 2. If you have a dial tone, check for DTMF voice band tones, such as touch-tone detection. If the dial tone stops when you dial a digit, the voice port is probably configured properly.

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

Step 4. Use the **show voice port** command to make sure 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 the port is in a hung state. Use the **shutdown/no shutdown** command sequence to reinitialize the port.

Step 5. If you have configured E&M interfaces, make sure the values associated with your specific PBX setup are correct. Specifically, check for two-wire or four-wire wink-start, immediate-start, or delay-start signaling types, and the E&M interface type. These parameters need to match those set on the PBX for the interface to communicate properly.

Step 6. You must confirm that the voice network module (VNM) (that is, the module in the router that contains the voice ports) 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 whether the problem is with the VIC card or with the module slot.

For your reference, Table 3-6 lists six **show** commands for verifying the voice-port configuration.

Table 3-6 *Commands to Verify Voice Ports*

Command	Description
show voice port	Shows all voice-port configurations in detail
show voice port *slot/subunit/port*	Shows one voice-port configuration in detail
show voice port summary	Shows all voice-port configurations in brief
show voice busyout	Shows all ports configured as busyout
show voice dsp	Shows status of all DSPs
show controller T1 | E1	Shows the operational status of a controller

Example 3-7 provides sample output for the **show voice port** command.

Example 3-7 show voice port *Command*

```
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
```

Example 3-8 provides sample output for the **show voice port summary** command.

Example 3-8 show voice port summary *Command*

```
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
```

For your further reference, Table 3-7 provides a series of commands used to test Cisco voice ports. The **test** commands provide the capability to analyze and troubleshoot voice ports on voice-enabled routers. As Table 3-7 shows, you can use five **test** commands to force voice ports into specific states to test the voice port configuration. The **csim start** *dial-string* command simulates a call to any end station for testing purposes.

Table 3-7 test *Commands*

Command	Description
test voice port *port_or_DS0-group_identifier* **detector {m-lead | battery-reversal | ring | tip-ground | ring-ground | ring-trip} {on | off | disable}**	Forces a detector into specific states for testing.
test voice port port_or_*DS0-group_identifier* **inject-tone** {**local** | **network**} {**1000hz** | **2000hz** | **200hz** | **3000hz** | **300hz** | **3200hz** | **3400hz** | **500hz** | **quiet** | **disable**}	Injects a test tone into a voice port. A call must be established on the voice port under test. When you are finished testing, be sure to use the **disable** option to end the test tone.
test voice port *port_or_DS0-group_identifier* **loopback** {**local** | **network** | **disable**}	Performs loopback testing on a voice port. A call must be established on the voice port under test. When you finish the loopback testing, be sure to use the **disable** option to end the forced loopback.
test voice port *port_or_DS0-group_identifier* **relay** {**e-lead** | **loop** | **ring-ground** | **battery-reversal** | **power-denial** | **ring** | **tip-ground**} {**on** | **off** | **disable**}	Tests relay-related functions on a voice port.
test voice port *port_or_DS0-group_identifier* **switch** {**fax** | **disable**}	Forces a voice port into fax or voice mode for testing. If the voice port does not detect fax data, the voice port remains in fax mode for 30 seconds and then reverts automatically to voice mode. After you enter the **test voice port switch fax** command, you can use the **show voice call** command to check whether the voice port is able to operate in fax mode.
csim start *dial-string*	Simulates a call to the specified dial string. This command is most useful when testing dial plans.

Introducing Dial Peers

As a call is set up across the network, the existence of various parameters is checked and negotiated. A mismatch in parameters can cause call failure. Therefore, 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. A network designer needs in-depth knowledge of dial-peer configuration options and their uses. This section discusses the proper use of digit manipulation and the configuration of dial peers.

Understanding Call Legs

Call legs are logical connections between any two telephony devices, such as gateways, routers, Cisco Unified Communication Managers, or telephony endpoint devices. Additionally, 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 topology shown in Figure 3-23 illustrates the four call legs involved in an end-to-end call between two voice-enabled routers.

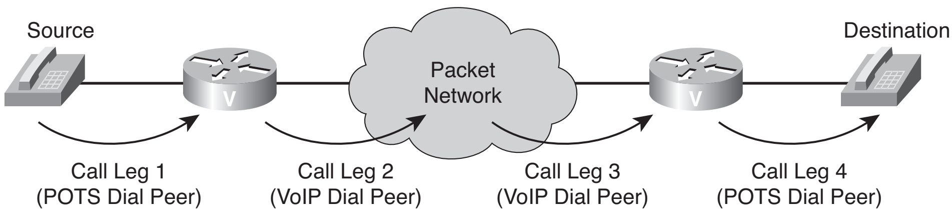

Figure 3-23 *Dial Peers and Call Legs*

An end-to-end call consists of four call legs: two from the source router's perspective and two from the destination router's perspective. To complete an end-to-end call from either side and send voice packets back and forth, you must configure all four dial peers. Dial peers are used only to set up calls. After the call is established, dial peers are no longer employed.

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, as depicted in Figure 3-24.

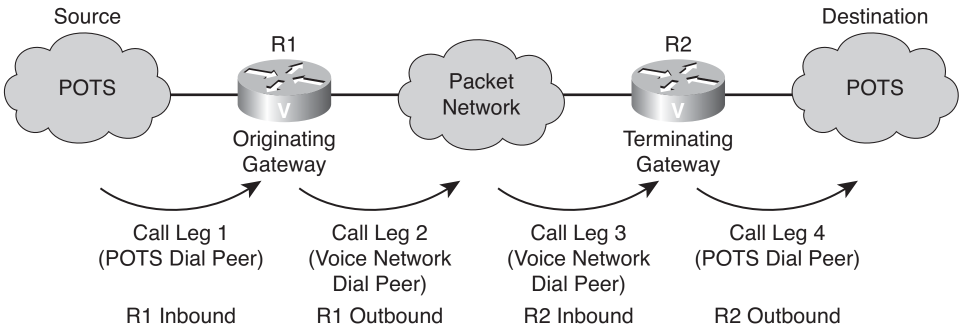

Figure 3-24 *End-to-End Calls*

A call is segmented into call legs, and a dial peer is associated with each call leg. The process for call setup, as diagrammed in Figure 3-24, is the following:

- The POTS call arrives at R1, and an inbound POTS dial peer is matched.
- After associating the incoming call to an inbound POTS dial peer, R1 creates an inbound POTS call leg and assigns it a call ID (call leg 1).
- R1 uses the dialed string to match an outbound VoIP dial peer.
- After associating the dialed string to an outbound voice network dial peer, R1 creates an outbound voice network call leg and assigns it a call ID (call leg 2).
- The voice network call request arrives at R2, and an inbound VoIP dial peer is matched.
- After R2 associates the incoming call to an inbound VoIP dial peer, R2 creates the inbound voice network call leg and assigns it a call ID (call leg 3). At this point, both R1 and R2 negotiate voice network capabilities and applications, if required. The originating router or gateway might request nondefault capabilities or applications. When this is the case, the terminating router or gateway must match an inbound VoIP dial peer that is configured for such capabilities or applications.
- R2 uses the dialed string to match an outbound POTS dial peer.
- 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).

Understanding Dial Peers

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

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

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

Cisco voice-enabled routers support five types of dial peers, including POTS, VoIP, Voice over Frame Relay (VoFR), Voice over ATM (VoATM), and Multimedia Mail over IP (MMoIP). However, this book focuses on POTS and VoIP dial peers, which are the fundamental dial peers used in constructing a VoIP network:

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

In Figure 3-25, the telephony device connects to the Cisco voice-enabled router. The POTS dial-peer configuration includes the telephone number of the telephony device and the voice port to which it is attached. The router determines where to forward incoming calls for that telephone number.

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

Follow these steps to enable a router to complete a VoIP call:

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

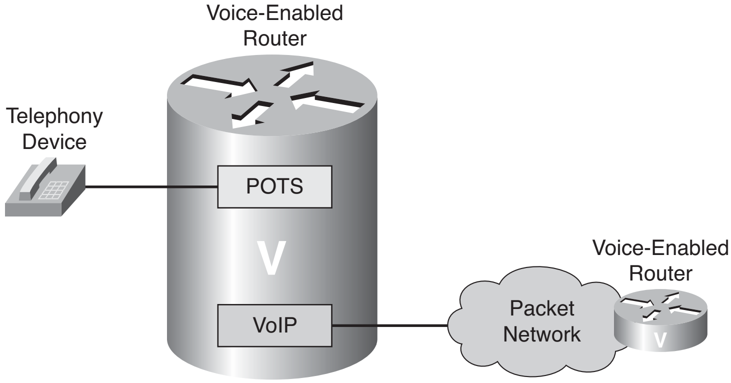

Figure 3-25 *Dial Peers*

Configuring POTS Dial Peers

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

Follow 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.

Step 2. Use the **destination-pattern** command in dial-peer configuration mode to configure the telephone number.

Step 3. Use the **port** command in dial-peer configuration mode to specify the physical voice port that the POTS telephone is connected to.

The dial-peer type will be specified as POTS because the edge device is directly connected to a voice port, and the signaling must be sent from this port to reach the device. Two basic parameters 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.

Figure 3-26 shows a POTS dial peer. Example 3-9 illustrates proper POTS dial-peer configuration on the Cisco voice-enabled router shown in Figure 3-26. The **dial-peer voice 1 pots** command notifies the router that dial peer 1 is a POTS dial peer with a tag of 1. The tag is a number that is locally significant to the router. Although the tag does not need to match the phone number specified by the **destination-pattern** command, many administrators recommend configuring a tag that does match a dial-peer's phone number to help make the configuration more intuitive. The **destination-pattern** *7777* command notifies the router that the attached telephony device terminates calls destined for telephone number 7777. The **port 1/0/0** command notifies the router that the telephony device is plugged into module 1, VIC slot 0, and voice port 0.

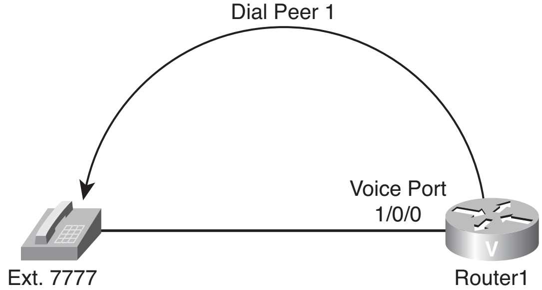

Figure 3-26 *POTS Dial Peer*

Example 3-9 *Configuration for Dial Peer 1 on Router 1*

```
Router1#configure terminal
Router1(config)#dial-peer voice 1 pots
Router1(config-dialpeer)#destination-pattern 7777
Router1(config-dialpeer)#port 1/0/0
Router1(config-dialpeer)#end
```

Practice Scenario 1: POTS Dial Peer Configuration

To practice the configuration of a POTS dial peer, consider a scenario. In this scenario, assume that a data center exists at the R1 site and executive offices at the R2 site. Using the diagram shown in Figure 3-27, create POTS dial peers for the four telephones shown.

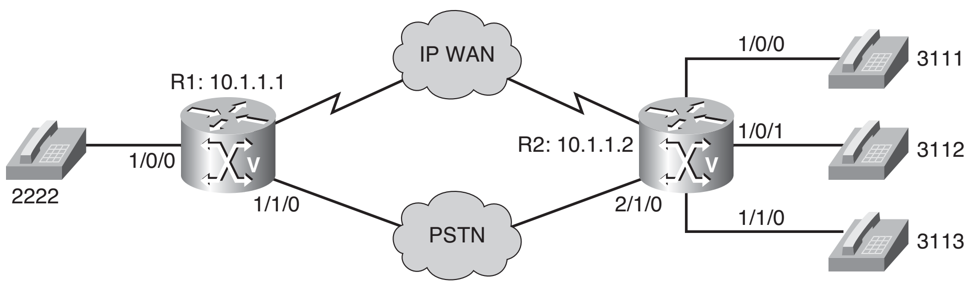

Figure 3-27 *Practice Scenario 1*

Note that three configuration commands are required for R1, and nine configuration commands are required for R2. You can write the commands in the space provided here or use a separate sheet of paper. The suggested solution follows.

R1:

____

____

____

R2:

Practice Scenario 1 Suggested Solution

Although your choice of dial-peer tags might vary, the following offers a suggested solution to Practice Scenario 1:

R1:

```
dial-peer voice 2222 pots
        destination-pattern 2222
        port 1/0/0
```

R2:

```
dial-peer voice 3111 pots
        destination-pattern 3111
        port 1/0/0
dial-peer voice 3112 pots
        destination-pattern 3112
        port 1/0/1
dial-peer voice 3113 pots
        destination-pattern 3113
        port 1/1/0
```

Configuring VoIP Dial Peers

The administrator must know how to identify the far-end voice-enabled device that will terminate the call. In a small network environment, the device might be the IP address of the remote device. In a large environment, identifying the device might mean pointing to a Cisco Unified Communications Manager or gatekeeper for address resolution and CAC to complete the call.

Follow these steps to configure VoIP dial peers:

Step 1. Configure the path across the network for voice data.

Step 2. Specify the dial peer as a VoIP dial peer.

Step 3. Use the **destination-pattern** command to configure a range of numbers reachable by the remote router or gateway.

Step 4. Use the **session target** command to specify the IP address of the terminating router or gateway.

Step 5. (Optional) As a best practice, use the remote device loopback address as the IP address.

The dial peer specified as a VoIP dial peer alerts the router that it must process a call according to the various dial-peer parameters. The dial peer must then send the call setup information in IP packets for transport across the network. Specified parameters might include the codec used for compression (for example, VAD) or marking the packet for priority service.

The **destination-pattern** parameter configured for this dial peer is typically a range of numbers reachable via the remote router or gateway.

Because this dial peer points to a device across the network, the router needs a destination IP address to put in the IP packet. The **session target** parameter allows the administrator to specify either an IP address of the terminating router or gateway or another device. For example, a gatekeeper or Cisco Unified Communications Manager might return an IP address of that remote terminating device.

To determine which IP address a dial peer should point to, Cisco recommends 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 an alternate path to the router exists.

Figure 3-28 shows a topology needing a VoIP dial peer configured on Router1. Example 3-10 lists the proper VoIP dial-peer configuration on Router 1, which is a Cisco voice-enabled router. The **dial-peer voice 2 voip** command notifies the router that dial peer 2 is a VoIP dial peer with a tag of 2. The **destination-pattern 8888** command notifies the router that this dial peer defines an IP voice path across the network for telephone number 8888. The **session target ipv4:10.18.0.1** command defines the IP address of the router connected to the remote telephony device.

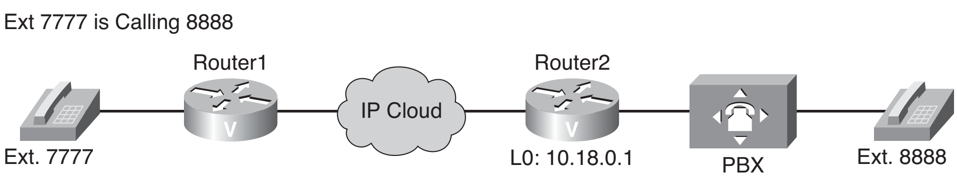

Figure 3-28 *VoIP Dial Peers*

Example 3-10 *Configuration for Dial Peer 2 on Router 1*

```
Router1#configure terminal
Router1(config)#dial-peer voice 2 voip
Router1(config-dialpeer)#destination-pattern 8888
Router1(config-dialpeer)#session target ipv4:10.18.0.1
Router1(config-dialpeer)#end
```

Practice Scenario 2: VoIP Dial Peer Configuration

Create VoIP dial peers for each of the R1 and R2 sites based on the diagram presented in Figure 3-29.

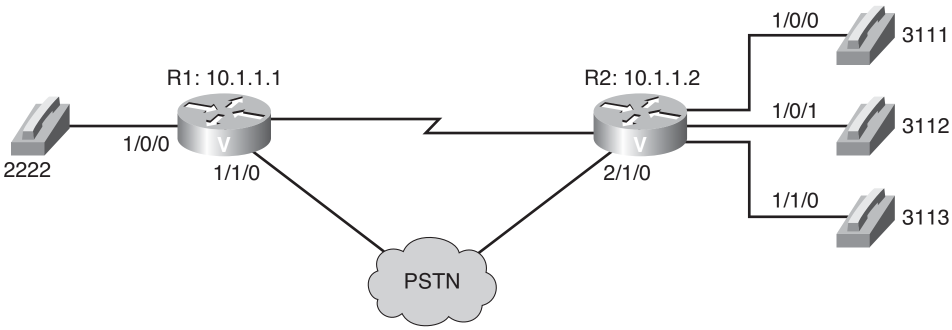

Figure 3-29 *Practice Scenario 2*

R1:

____

____

____

____

____

____

____

____

____

R2:

____

____

____

Practice Scenario 2 Suggested Solution

Although your choice of dial-peer tags might vary, the following offers a suggested solution to Practice Scenario 2:

R1:

```
dial-peer voice 3111 voip
       destination-pattern 3111
       Session target ipv4:10.1.1.2
dial-peer voice 3112 voip
       destination-pattern 3112
       Session target ipv4:10.1.1.2
dial-peer voice 3113 voip
       destination-pattern 3113
       Session target ipv4:10.1.1.2
```

R2:

```
dial-peer voice 2222 voip
       destination-pattern 2222
       Session target ipv4:10.1.1.1
```

From this practice scenario, notice how configuration intensive it would be for an administrator to configure a dial peer for each phone number in a VoIP network. Next, consider how wildcards can be used with the **destination-pattern** command to allow a single dial peer to point to multiple phone numbers.

Configuring Destination Pattern Options

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 configured as the destination pattern for the voice-telephony peer. It also determines the dialed digits 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 (using the **prefix** *digits* command), 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.

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, which has the following syntax:

```
destination-pattern [+] string [T]
```

Destination-pattern options include the following:

- **Plus sign (+):** An optional character that indicates an E.164 standard number. E.164 is the International Telecommunication Union Telecommunication Standardization sector (ITU-T) recommendation for the international public telecommunication numbering plan. The plus sign in front of a destination-pattern string specifies that the string must conform to E.164.
- ***string*:** A series of digits specifying the E.164 or private dial-plan telephone number. The following examples show the use of special characters often found in destination pattern strings:
  - **Asterisk (*) and pound sign (#):** An asterisk (*) and pound sign (#) appear on standard touch-tone dial pads. These characters might need to be used when passing a call to an automated application that requires these characters to signal the use of a special feature. For example, when calling an interactive voice response (IVR) system that requires a code for access, the number dialed might be 5551212888#, which would initially dial the telephone number 5551212 and input a code of 888 followed by the pound key to terminate the IVR input query.
  - **Comma (,):** A comma (,) inserts a one-second pause between digits. The comma can be used, for example, where a 9 is dialed to signal a PBX that the call should be processed by the PSTN. The 9 is followed by a comma to give the PBX time to open a call path to the PSTN, after which the remaining digits are played out. An example of this string is 9,5551212.
  - **Period (.):** 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 might be accessible via a single destination router, gateway, PBX, or Cisco Unified Communications Manager. A pattern of **200.** allows for ten uniquely addressed devices, whereas 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, a bracket notation would be more efficient, as described next.

- **Brackets ([ ]):** Brackets ([ ]) indicate a range. A range is a sequence of characters enclosed in the brackets. Only single numeric characters from 0 through 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 pattern of **20[0–4].** would be used for the first site, and a pattern of **20[5–9].** would be used for the second site. Note that in both cases, a dot is used in the last digit position to represent any single digit from 0 through 9. The bracket notation offers much more flexibility in how numbers can be assigned.

- **T**: An optional control character indicating that the **destination-pattern** value is a variable-length dial string. In cases where callers might 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 have a varying number of dialed digits. A single dial peer with a destination pattern of **.T** could support the different call types. The **interdigit timeout** determines when a string of dialed digits is complete. The router continues to collect digits until there is an interdigit pause longer than the configured value, which by default is 10 seconds.

- However, 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 might 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.

Table 3-8 demonstrates the use of various destination pattern wildcards, including the period, brackets, and the **.T** wildcards.

Table 3-8 *Destination Pattern Options*

Destination Pattern	Matching Telephone Numbers
5550124	Matches one telephone number exactly, 5550124. This is typically used when a single device, such as a telephone or fax, is connected to a voice port.

Table 3-8 *Destination Pattern Options (continued)*

Destination Pattern	Matching Telephone Numbers
55501[1-3].	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 type of destination pattern is used when telephone number ranges are assigned to specific sites. In this example, the destination pattern is used in a small site that does not need more than 30 numbers assigned.
.T	Matches any telephone number that has at least one digit and can vary in length from 1 through 32 digits total. This destination pattern is used for a dial peer that services a variable-length dial plan, such as local, national, and international calls. It can also be used as a default destination pattern so 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

When determining how inbound dial peers are matched on a router, it is important to note whether the inbound call leg is matched to a POTS or VoIP dial peer. Matching occurs in the following manner:

- Inbound POTS dial peers are associated with the incoming POTS call legs of the originating router or gateway.
- Inbound VoIP dial peers are associated with the incoming VoIP call legs of the terminating router or gateway.

Three information elements sent in the call setup message are matched against four configurable **dial-peer** command attributes. Table 3-9 describes the three call setup information elements.

Table 3-9 *Call Setup Information Elements*

Call Setup Element	Description
Called number dialed number identification service	This is the call-destination dial string, and it is derived from the ISDN setup message or channel associated signaling (CAS) DNIS.
Calling number automatic number identification	This is a number string that represents the origin, and it is derived from the ISDN setup message or CAS ANI. The ANI is also referred to as the calling line ID (CLID).
Voice port	This represents the POTS physical voice port.

The four configurable **dial-peer** command attributes are detailed in Table 3-10.

Table 3-10 *Command Attributes for the* **dial-peer** *Command*

dial-peer Command Attribute	Description
incoming called-number	Defines the called number or DNIS string.
answer-address	Defines the originating calling number or ANI string.
destination-pattern	Uses the calling number (originating or ANI string) to match the incoming call leg to an inbound dial peer.
Port	Attempts to match the configured dial peer port to the voice port associated with the incoming call (POTS dial peers only).

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 following order:

1. The router or gateway attempts to match the called number of the call setup request with the configured **incoming called-number** of each dial peer.
2. If a match is not found, the router or gateway attempts to match the calling number of the call setup request with the **answer-address** of each dial peer.
3. If a match is not found, the router or gateway attempts to match the calling number of the call setup request to the **destination-pattern** of each dial peer.
4. The voice port uses the voice port number associated with the incoming call setup request to match the inbound call leg to the configured dial peer **port** parameter.

5. If multiple dial peers have the same port configured, the router or gateway matches the first dial peer added to the configuration.
6. If a match is not found in the previous steps, dial peer 0 is matched.

Because call setups always include DNIS information, you should use the **incoming called-number** command for inbound dial peer matching. Configuring **incoming called-number** is useful for a company that has a central call center providing support for a number of different products. Purchasers of each product get a unique 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** is useful when you want to match calls based on the originating calling number. For example, when a company has international customers who require foreign-language-speaking agents to answer the call, the call can be routed to the appropriate agent based on the country of call origin.

You must use the calling number ANI with **destination-pattern** when the dial peers are set up for two-way calling. In a corporate environment, the head office and remote sites must be connected. As long as each site has a VoIP dial peer configured to point to each site, inbound calls from each remote site will match against that dial peer.

Characteristics of the Default Dial Peer

When a matching inbound dial peer is not found, the router resorts to a virtual dial peer called the *default dial peer*. The default dial peer is often referred to as *dial peer 0*.

> **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.

Dial peer 0 for inbound VoIP peers has the following characteristics:

- Any codec
- IP precedence 0
- VAD enabled
- No RSVP support
- **fax-rate** service

For inbound POTS peers, dial peer 0 is configured with the **no ivr application** command.

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 might have different parameters from the voice path in the return direction. This might 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. Interestingly, the default dial peer cannot be viewed using **show** commands.

In Figure 3-30, only one-way dialing is configured. Example 3-11 and Example 3-12 illustrate the configuration for this topology. The caller at extension 7777 can call extension 8888 because a VoIP dial peer is configured on Router 1 to route the call across the network. However, no VoIP dial peer is configured on Router 2 to point calls across the network toward Router 1. Therefore, no dial peer exists 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).

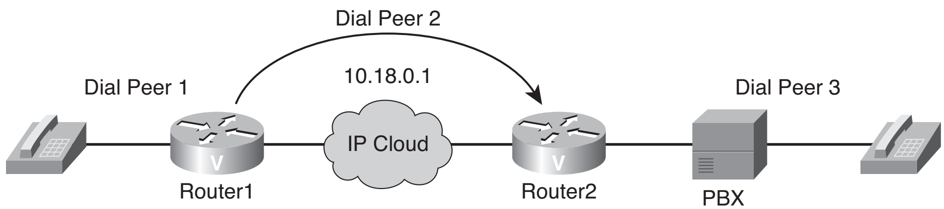

Figure 3-30 *Default Dial Peer 0*

Example 3-11 *Router 1 Configuration*

```
Router1(config)#dial-peer voice 1 pots
Router1(config-dial-peer)#destination-pattern 7777
Router1(config-dial-peer)#port 1/0/0
Router1(config-dial-peer)#exit
Router1(config)#dial-peer voice 2 voip
Router1(config-dial-peer)#destination-pattern 8888
Router1(config-dial-peer)#session target ipv4:10.18.0.1
```

Example 3-12 *Router 2 Configuration*

```
Router2(config)#dial-peer voice 3 pots
Router2(config-dial-peer)#destination-pattern 8888
Router2(config-dial-peer)#port 1/1/0
```

Matching Outbound Dial Peers

Outbound dial-peer matching is completed on a digit-by-digit basis. Therefore, the router or gateway checks for dial-peer matches after receiving each digit and then routes the call when a full match is made.

The router or gateway matches outbound dial peers in the following order:

Step 1. The router or gateway uses the dial peer **destination-pattern** command to determine how to route the call.

Step 2. The **destination-pattern** command routes the call in the following manner:

- On POTS dial peers, the **port** command forwards the call.
- On VoIP dial peers, the **session target** command forwards the call.

Step 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.

In Example 3-13, 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 55501. Dial peer 4 matches the specific number 5550124 only. When the number 5550124 is dialed, dial peers 1, 3, and 4 all match that number, but dial peer 4 places that call because it contains the most specific destination pattern.

Example 3-13 *Matching Outbound Dial Peers*

```
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#destination-pattern .T
Router(config-dial-peer)#session target ipv4:10.1.1.1

Router(config)#dial-peer voice 2 voip
Router(config-dial-peer)#destination-pattern 55501[3-4].
Router(config-dial-peer)#session target ipv4:10.2.2.2

Router(config)#dial-peer voice 3 voip
Router(config-dial-peer)#destination-pattern 555012.
Router(config-dial-peer)#session target ipv4:10.3.3.3

Router(config)#dial-peer voice 4 voip
Router(config-dial-peer)#destination-pattern 5550124
Router(config-dial-peer)#session target ipv4:10.4.4.4
```

Summary

The main topics covered in this chapter are the following:

- A VoIP network has seven typical call types.
- 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 directly connected to a voice-enabled router or PBX to gain access to the PSTN.
- Voice port call types include local, on-net, off-net, PLAR, PBX to PBX, intercluster trunk, and on-net to off-net calls.
- 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 analog circuits in telephony networks.
- FXS, FXO, and E&M ports have several configuration parameters.
- 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 a voice port.
- The **show**, **debug**, and **test** commands are used for monitoring and troubleshooting voice functions in the network.
- Dial peers are used to identify call source and destination endpoints and to define the characteristics applied to each call leg in the call connection.
- An end-to-end voice call consists of four call legs.
- A dial peer is an addressable call endpoint.
- POTS dial peers retain the characteristics of a traditional telephony network connection.
- 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 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.

Chapter Review Questions

The answers to these review questions are in the appendix.

1. If a client picked up a customer service handset and was automatically connected to a customer service representative without dialing any digits, what kind of call would it be?

- **a.** Intercluster trunk call
- **b.** PBX-to-PBX call
- **c.** On-net call
- **d.** PLAR call

2. Which configuration parameter would you change to set the dial tone, busy tone, and ringback tone on an FXS port?

- **a.** Cptone
- **b.** Ring frequency
- **c.** Ring cadence
- **d.** Description
- **e.** Signal
- **f.** PSQM

3. What is the default (and most commonly used) method of access signaling used on E&M voice ports?

- **a.** Immediate-start
- **b.** Wink-start
- **c.** Delay-start
- **d.** Loop-start

4. Which situation most likely requires changes to the FXS port default settings?

- **a.** The caller and the called party are in different parts of the country.
- **b.** The caller and the called party are in different countries.
- **c.** The connection is a trunk to a PBX.
- **d.** The FXS port configuration does not match the local PSTN switch configuration.

5. Which two conditions can be checked by using the **show voice port** *port* command for an FXS port? (Choose 2.)
   a. Whether the port is using ground-start or loop-start signaling
   b. The ring frequency configured for the port
   c. The E&M signaling type configured for the port
   d. The number of rings after which the port will answer
6. When an end-to-end call is established across a VoIP network, how many inbound call legs are associated with the call?
   a. One
   b. Two
   c. Three
   d. Four
7. A POTS dial peer performs which of the following two functions? (Choose 2.)
   a. Provides a phone number for the edge network or device
   b. Provides a destination address for the edge device located across the network
   c. Routes a call across a network
   d. Identifies the specific voice port that connects the edge network or device
8. When configuring a VoIP dial peer, which command is used to specify the address of the terminating router or gateway?
   a. **destination-port**
   b. **destination-pattern**
   c. **session target**
   d. **destination address**
   e. **dial-peer terminal**
9. What happens if there is no matching dial peer for an outbound call?
   a. The default dial peer is used.
   b. Dial peer 0 is used.
   c. The POTS dial peer is used.
   d. The call is dropped.

10. Which dial-peer configuration command attempts to match the calling number (that is, the ANI string)?

- **a.** **destination-pattern**
- **b.** **port**
- **c.** **answer-address**
- **d.** **incoming called-number**

Index

Numerics

2 B + D, 192
23 B + D, 192
30 B + D, 192
911 services, 357-358

A

a-law, 85
acceptable delay, G.114 recommendation, 59
ad hoc multipoint conferences, 262
addressing, SIP, 302-303
Admission messages (RAS), 453-455
AES (Advanced Encryption Standard), 20
ALI (Automatic Location Identification), 357
analog address signaling, 139
analog gateways, 22
analog signaling, 135-138
analog trunks, 152-154
  CAMA, 154-157
analog voice ports, 133-144
  E&M voice ports, configuring, 148-150
  FXO voice ports, configuring, 146-148
  FXS voice ports, configuring, 144, 146
ANI (Automatic Number Identification), 357
  dial peer matching, configuring, 402-403
application mgcpapp command, 287
associate ccm priority command, 118
associate profile register command, 119
associate profile sccp command, 116
audio codecs, 10
audio conferencing, 92
availability, five nines, 15

B

background noise, 56
bandwidth
  calculating total bandwidth for calls, 88-90
  capacity planning, 85
  Layer 2 overhead requirements, 88
  requirements, calculating, 88-90
  security and tunneling overhead, 88
  VAD, effect on, 90-91
  voice samples, effect on, 87-88
bandwidth command, 508
bearer channels, 8

bind interface command, 119
Blast LRQ messages (RAS), 459-460
BRI (Basic Rate Interface), 186, 193-194
BRI backhaul, 11
business case for VoIP, 4-6
busy tone, 140

C

CA-controlled mode (MGCP T.38 fax relay), 82
CAC (Call Admission Control), 504
  zone bandwidth, 506-508
calculating
  delay budget, 59
  DSP requirements, 103-106
  total bandwidth for calls, 88-90
  zone bandwidth, 506-507
call agents, 8
call coverage, 322, 326
call disconnect (RAS), 463
caller ID number manipulation, 377
call establishment, H.323, 258
call flows
  on Cisco UBE, 533, 537-538
  for gatekeepers, 464-468
  MGCP, 283-284
  SIP, 299-302
call legs, 164-165
call routing, 322, 325, 397
  configuring, 471-479
call setup, H.323, 260
caller ID number manipulation, 378-379
calling privileges, 322, 326. *See also* CoR (Class of Restriction)
CAMA (Centralized Automated Message Accounting) trunks, 154, 156-157, 358
capacity planning, 85
  Layer 2 overhead requirements, 88
  security and tunneling overhead, 88
  total bandwidth, calculating, 88-90
  voice samples, effect on bandwidth, 87-88
CAs, MGCP, 277-279
CAS (channel associated signaling), 187
  E1 R2 CAS, 189
  T1 CAS, 188
    configuring, 208-218
cause IE, 200
CBWFQ (Class-Based Weighted Fair Queuing), 65
CCS (common channel signaling), 187, 194
centralized multipoint conferences, 261

Cisco 827-4V ADSL router, 32
Cisco 1751-V Modular Access Router, 27
Cisco 1760-V Modular Access Router, 27
Cisco 2600XM Series multiservice routers, 28
Cisco 2800 Series Integrated Services Routers, 24
Cisco 3600 Series multiservice routers, 29
Cisco 3700 Series multiservice routers, 29
Cisco 3800 Series Integrated Services Routers, 25
Cisco 7200 Series routers, 34
Cisco AS5400 Series Universal gateways, 31
Cisco AS5850 Series Universal gateways, 31
Cisco VG200 Series gateways, 30
Cisco ATA 186, 33
Cisco Catalyst 6500 Series Switches, 26
Cisco Fax Relay, 66, 76-77
Cisco IOS gateways, codecs supported, 85-86
Cisco IOS routers, Cisco UBE support, 523
Cisco UBE (Unified Border Element), 521-523
call flows, 533, 537-538
Cisco IOS image support, 523
codec filtering, 530
configuring, 538
gatekeeper interworking, 532
H.323-to-H.323 interworking, configuring, 539
H.323-to-SIP interworking, configuring, 541-542
in enterprise environments, 523-526
media flows, 528-529
protocol interworking, 526
RSVP-based CAC, 530
transparent codec pass-through, configuring, 543
via-zone gatekeepers, configuring, 544-548
Cisco Unified Communication
QoS, 63
Cisco Unified Communications System, 3-4
clustering over IP WAN deployment model, 48-50
conference bridges, configuring, 111
deployment models
multisite WAN with centralized call processing, 40-43
multisite WAN with distributed call processing, 45-47
single-site deployment model, 36-38
transcoders, configuring, 113
Cisco voice gateways
CoR, 421-422
behavior, example, 422-424
for CME, 426-432
configuring, 434
example, 425-426
for SRST, 426, 433-434
clarity, factors affecting
delay, 57
jitter, 57
packet loss, 60

CLASS (Custom Local Area Subscriber Services), 276

CLECs (Competitive Local-Exchange Carriers), 276

clid commands, 377

clipping, 42

clustering over IP WAN deployment model, 48-50

CME (Cisco CallManager Express), CoR, 426-432

CMM (Cisco Communication Media Module), 27

codec complexity, 95-97

codec pass-through command, 116

codec preference command, 265

codec transparent command, 542

codecs, 8, 85

- Cisco IOS gateways, supported codecs, 85-86
- configuring on H.323 gateways, 265-266
- filtering on Cisco UBE, 530

commands

- application mgcpapp, 287
- ip rtp header-compression, 270
- mgcp call-agent, 285
- associate ccm priority, 118
- associate profile register, 119
- associate profile sccp, 116
- bandwidth, 508
- bind interface, 119
- clid, 377
- codec pass-through, 116
- codec preference, 265
- codec transparent, 542
- debug, 293
- debug isdn q921, 240
- debug isdn q931, 204, 240-242, 345
- debug voice translation, 347-348
- debug voip dialpeer, 346
- destination-pattern, 370
- dialplan-pattern, 390-392
- digit-srip, 368
- ds0-group, 187
- dsp services dspfarm, 115
- dspfarm profile, 115
- dtmf-relay, 273
- fax protocol, 270
- forward-digits, 368
- maximum sessions, 116
- num-exp, 368
- prefix, 368
- sccp, 117
- sccp ccm group, 118
- sccp ccm identifier, 117
- sccp local, 117
- show call active voice, 229
- show call history voice, 230-232
- show call resource voice threshold, 512
- show ccm-manager, 291
- show controller t1, 227
- show controllers, 239
- show dial-peer voice, 341
- show dialplan number, 341, 378-379
- show dspfarm profile, 119-120
- show gatekeeper endpoints, 487, 515
- show gateway, 274, 514
- show isdn status, 239
- show mgcp, 290
- show mgcp endpoint, 292
- show sip-ua calls, 311

show voice call summary, 228
show voice dsp, 228
show voice port summary, 226
station-id, 377
voice card, 115
voice port timing parameters, 159-160
voice-class codec, 265

comparing
voice-quality measurement methods, 62-63
VoIP signaling protocols, 12, 14

components of VoIP networks, 7

conference bridges, 93
configuring, 111

conferencing, configuring on voice gateways, 107-109

configuring
Cisco UBE
H.323-to-H.323 interworking, 539
H.323-to-SIP interworking, 541-542
analog voice ports
E&M voice ports, 148-150
FXO voice ports, 146-148
FXS voice ports, 144-146
Cisco UBE, 538
transparent codec pass-through, 543
via-zone gatekeepers, 544- 548
codec complexity, 96-97
conferencing on voice gateways, 107-109
CoR
for CME, 427-432
for SRST, 433-434
destination patters, 172-174
dial peers
for H.323 gatekeepers, 500-502
H.323, 405-406
POTS, 167-169
VoIP, 169-172
DID trunks, 157-159
digit manipulation, 367-369, 393-395
translation rules, 396-397
DSP farms, 107-109, 114-115
verifying configuration, 119-120
E1 R2 trunks, 218-220
gatekeepers, 489-490
call routing, 471-479
directory gatekeepers, 479-486
RAI, 511-512
technology prefixes, 469-471, 495-497
verifying configuration, 487-488
zone prefixes, 468-469, 494
zones, 493
gateways for H.323 gatekeepers, 497-500
H.323, 247-251, 254, 263-264, 268
codecs, 265-266
DTMF relay, 273-274
fax pass-through, 269-270
fax relay, 271-272
gatekeepers, 256-258
terminals, 254
timers, 267
UBEs, 255-256
verifying configuration, 274-275
inbound site-code dialing, 416
ISDN trunks, 220-225

MGCP, 285
fax relay, 288-290
RGWs, 285-286
TGWs, 286
verifying configuration, 290-293
outbound site-code dialing, 415-416
PSTN dial plans, 331-340
QSIG, 236
over BRI, 238
over PRI, 236-237
SCCP, 109, 116-119
SIP, 306-308
verifying configuration, 309-314
site-code dialing, 410-414
T1 CAS trunks, 208
controller settings, 208-215
digital voice port parameters, 215-216
inbound and outbound ANI, 216-218
TEHO, 417-419
toll-bypass, 410-414
transcoding on voice gateways, 107-109
voice ports
timing parameters, 159-160
verifying configuration, 160-163
zone bandwidth, 508
congestion tone, 140
control commands
MGCP, 280-282
controller setting, configuring on T1 CAS trunks, 208-211, 213, 215
CoR (Class of Restriction), 421-422
behavior, example, 422-424
for CME, 426-432
example, 425-426
for SRST, 426, 433-434
verifying, 434
corlists, 421-422
CoS (Class of Service), 64
CP (call progress) tones, 139-140
cRTP (Compressed RTP), 18-20

D

database services, 8
debug commands, 293
debug isdn q921 command, 240
debug isdn q931 command, 204, 240-242, 345
debug voice translation command, 347-348
debug voip dialpeer command, 346
default dial peer, characteristics, 177-178
delay, 56-57
delay budget, calculating, 59
delay-start signaling, 144
deployment models
clustering over IP WAN, 48-50
multisite WAN with centralized call processing, 39-43
multisite WAN with distributed call processing, 43-47
single-site, 36-38
designing
large-scale dial plans, 326, 328
numbering plans, private, 349
destination patters, 166
configuring, 172-174
destination-pattern command, 370

dial peers, 164-166, 398
configuring for H.323 gatekeepers, 500-502
default dial peer, characteristics, 177-178
destination patterns, configuring, 172-174
H.323, configuring, 405-406
inbound matching process, 175-177
outbound matching process, 179
POTS, 166
configuring, 167-169
digit manipulation, 375
VoIP, 166
configuring, 169-172
dial plan-pattern command, 390-392
dial plans, 321, 323
call coverage, 326
call routing, 325
calling privileges, 326
components of, 322
digit manipulation, 325
configuring, 393-397
voice translation, 380-393
endpoint addressing, 324
example, 360-361
ISDN, 330
large-scale
designing, 326-328
path selection, 325
PSTN
configuring, 331-340
inbound calls, 329
outbound calls, 329
requirements, 328
verifying, 341-348
dial tone, 140
dial-peer matching, 398-400
ANI matching, 402-403
DNIS matching, 402-403
in hunt groups, 404
inbound, 401
outbound, 402
DID (Direct Inward Dial) trunks, 22
configuring, 157-159
digit collection, example, 371
digit consumption, 370
digit forwarding, 372
digit manipulation, 322, 325
caller ID number manipulation, 377-379
configuring, 367-369, 393-395
for POTS dial peers, 375
number expansion, 374-375
example, 376-377
order of operation, 369
translation rules, configuring, 396-397
voice translation, 380-381
profiles, 385-392
rules, 382-384, 392-393
digit prefixing, 373
digit stripping, 371
digit-strip command, 368
digital gateways, 22
digital trunks, 186
E1 R2, 187-189, 218-220
ISDN, 191
BRI interfaces, 193-194
configuring, 220- 225
IEs, 200-205
media types, 191-193
messages, 198-199

PRI interfaces, 193-194
Q.921 signaling, 195
Q.931 signaling, 195-198
QSIG, verifying, 239-242
T1 CAS, configuring, 187-188, 208-218
digital voice ports
parameters, configuring on T1 CAS trunks, 215-216
verifying, 225-232
directory gatekeepers, configuring, 479, 481-486
display IE, 202
distributed multipoint conferences, 262
DNIS matching on dial peers, configuring, 402-403
DS0 (digital signal level 0), 187
ds0-group command, 187
DSP farms
configuring, 107-109, 114-115
verifying configuration, 119-120
DSP profiles, creating, 108-109
dsp services dspfarm command, 115
dspfarm profile command, 115
DSPs (Digital Signal Processors), 55
requirements, 98, 101-106
DTMF (Dual Tone Multifrequency), 23
H.323, 83, 273-274
SIP, 83-84, 304-305
dtmf-relay command, 273

E

E&M signaling, 134, 140
physical interface, 142
voice ports, configuring, 148-150
E.164 standard, 349
E1 R2 trunks, 187-189
configuring, 218-220
E1 voice circuits, 185
echo, 56
ELIN (Emergency Location Identification Number), 357
emergency 911 services, 357-358
endpoint addressing, 322-324
endpoints, MGCP, 277
enhanced media resources
DSPs, configuring, 114-115
SCCP, configuring, 116-119
enterprise networks, Cisco UBE, 523-526
ERL (Emergency Response Location), 357
ESF (Extended Super Frame) format, 188
examples
of digit collection, 371
of number expansion, 376-377
extended super frames, 187

F

f8-mode (AES), 20
facility IE, 201
failover, 48
fast connect call setup, H.323, 260
fax pass-through, 66-69, 75
fax protocol command, 270
fax relay, 66-69
H.323, configuring, 271-272
MGCP, configuring, 288-290

fax transmissions in IP networks, 66
Cisco Fax Relay, 76-77
fax pass-through, 67-69
fax relay, 69
H.323 T.38 fax relay, 77-79
MGCP T.38 fax relay, 80
modem pass-through, 69
SIP T.38 fax relay, 79-80
store-and-forward fax, 73
Feature Navigator tool, 445
features of Cisco UBE, 524-526
fidelity, 56
five nines, 15
flow encryption, 20
forward-digits command, 368
FRF.12, 63
FRTS (Frame Relay Traffic Shaping), 63
FXO voice ports, 134
configuring, 146-148
FXS voice ports, 133-305
configuring, 144-146

G

G.114 recommendation, 59
G.711 codecs, 85
G.723 codecs, 86
G.726 codecs, 85
G.728 codecs, 85
G.729 codecs, 85
Gatekeeper Discovery messages (RAS), 450-451
gatekeeper interworking on Cisco UBE, 532
gatekeepers, 441-442
CAC, 504
zone bandwidth, calculating, 506-507
zone bandwidth, configuring, 508
call routing, configuring, 471-479
configuration, verifying, 502-504
configuring, 489-490
dial peers, configuring, 500-502
directory gatekeepers, configuring, 479-486
H.323, 256-258
hardware and software requirements, 445
RAI, 510
configuring, 511-512
verifying operation, 512-515
signaling, 445
RAS, 446- 468
technology prefixes, 444
configuring, 469-471, 495-497
zone bandwidth, verifying, 509
zone prefixes, 444
configuring, 468-469, 493-494
gateway controlled mode (MGCP T.38 fax relay), 81
gateways, 21-23
Cisco 1751-V Modular Access Router, 27
Cisco 1760-V Modular Access Router, 27
Cisco 2600XM Series multiservice routers, 28
Cisco 2800 Series Integrated Services Routers, 24
Cisco 3600 Series multiservice routers, 29

Cisco 3700 Series multiservice routers, 29
Cisco 3800 Series Integrated Services Routers, 25
Cisco Catalyst 6500 Series Switches, 26
Cisco IOS gateways, supported codecs, 85-86
configuring to use H.323 gatekeepers, 497-500
H.323, 254
call establishment, 258
call setup, 260
configuring, 247, 249-251, 263-274
fast connect call setup, 260
gatekeepers, 256-258
multipoint conferences, 261
terminals, 254
UBEs, 255-256
verifying configuration, 274-275
MGCP, 275-278
call flows, 283-284
calls, 280
CAs, 279
configuring, 285-290
control commands, 280-282
packages, 282
verifying configuration, 290-293
SIP, 294-298
addressing, 302-303
call flow, 299-302
configuring, 306-308
DTMF relay, 304-305
verifying configuration, 309-314
standalone, 30
Cisco 7200 Series routers, 34
Cisco 827-4V ADSL router, 32
Cisco AS5300 Series Universal gateways, 31
Cisco AS5400 Series Universal gateways, 31
Cisco AS5850 Series Universal gateways, 31
Cisco ATA 186, 33
Cisco VG200 Series gateways, 30
GKRCS (Gatekeeper Route Control Server), 486
Ground-start signaling, 137-138
GSMF (GSM Full Rate Codec), 86
GUP (Gatekeeper Update Protocol), 445

H

H.225 call signaling, 10, 445
H.245 control function (H.323), 10, 249
DTMF, 83
H.323-to-H.323 interworking, configuring on Cisco UBE, 539
H.323-to-SIP interworking, configuring on Cisco UBE, 541-542
H.323, 9, 13, 254
call establishment, 258
call setup, 260
codecs, configuring, 265-266
configuring, 247-251, 263-264, 268
dial peers, configuring, 405-406
DTMF relay, 83, 273-274
fast connect call setup, 260
fax pass-through, configuring, 269-270
fax relay, configuring, 271-272

gatekeepers, 256-258, 441-442
CAC, 504-508
call flow, 464-468
call routing, 471-479
configuring, 489-490, 493-497
dial peers, configuring, 500, 502
directory gatekeepers, 479-486
hardware and software requirements, 445
RAI, 510-515
signaling, 445-463
technology prefixes, 444, 469-471
verifying, 487-488, 502-504
zone prefixes, 468-469
zones, 444
multipoint conferences, 261
supplementary services, 93
T.38 fax relay, 77-79
terminals, 254
timers, configuring, 267
UBEs, 255-256
verifying configuration, 274-275
H.324 terminals, 254
hardware MTPs, 92-94
header compression, 63
HMAC-SHA1 algorithm, 21
hunt groups, dial-peer matching, 404

I

IEs (information elements), 200-205
iLBC (Internet Low Bit Rate Codec), 86
ILECs (Incumbent Local-Exchange Carriers), 276
immediate-start signaling, 142
inbound ANI, configuring on T1 CAS trunks, 216, 218
inbound call legs, 164-165
inbound dial-peer matching, 175-177, 401
inbound ISDN calls, 330
inbound PSTN calls, 329
inbound site code dialing, configuring, 416
incoming call legs, 397
Information messages (RAS), 455
informational signaling, 139-140
integrating
internal and public numbering plans, 354
private and public numbering plans, 353
intercluster trunk calls, 129-130
international numbering plans, 349
interzone call setup, configuring, 462-463
intrazone call setup, configuring, 460
IP networks
fax transmissions, 66
Cisco Fax Relay, 76-77
fax pass-through, 67-69
fax relay, 69
H.323 T.38 fax relay, 77-79
MGCP T.38 fax relay, 80
modem pass-through, 69
SIP T.38 fax relay, 79-80
store-and-forward fax, 73
modem transmissions, modem relay, 71-73
ip rtp header-compression command, 270

IP telephony deployment models
clustering over IP WAN, 48-50
multisite WAN with centralized call processing, 40-43
multisite WAN with distributed call processing, 45-47
single-site, 36-38
ISDN, 186, 191
bearer capability values, 205
BRI interfaces, 193-194
cause code fields, 205
dial plans, 330
IEs, 200-205
inbound calls, 330
media types, 191-193
messages, 198-199
NFAS, 208
PRI interfaces, 193-194
Q.921 signaling, 195
Q.931 signaling, 195-198
trunks, configuring, 220- 225

J-K-L

jitter, 15, 56-58

large-scale dial plans, designing, 326-328
Layer 2 overhead requirements, 88
LLQ (Low Latency Queuing), 64
local calls, 125
local failover, 48
location messages (RAS), 456
location servers, 298
loop-start signaling, 136-137

M

mail system integration, SMDI, 22
matching dial peers, 398-400
ANI matching, 402-403
DNIS matching, 402-403
in hunt groups, 404
inbound dial peers, 175-177, 401
outbound dial peers, 179, 402
maximum sessions command, 116
MCU (Multipoint Control Unit), 7
measuring sound quality
MOS, 61
PESQ, 62
PSQM, 61
media flow around, 528
media flow-through, 528
media flows on Cisco UBE, 528-529
media resources, 91
conference bridges, configuring, 111
DSP requirements
calculating, 103-106
on NM-HDV, 98, 101-103
transcoders, configuring, 113
media transmission protocols, 16
messages, ISDN, 198-199
MGCP (Media Gateway Control Protocol), 13, 275-278
call flows, 283-284
calls, 280
CAs, 279
configuring, 285
control commands, 280-282
fax relay, configuring, 288-290
packages, 282

PRI/BRI backhaul, 11
RGWs, configuring, 285-286
T.38 fax relay, 80
TGWs, configuring, 286
troubleshooting, 293
verifying configuration, 290-293

mgcp call-agent command, 285

MLP (Multilink PPP), 64

MMUSIC (Multiparty Multimedia Session Control) Working Group, 12

modem pass-through, 69

modem relay, 71
gateway-controlled negotiation parameters, 73
jitter buffers, 73
payload redundancy, 72

MOS (mean opinion score), 61

MSAG (Master Street Address Guide), 357

MTP (media termination point), 92-93
hardware MTPs, 94
software MTPs, 94

mu-law, 85

multiframes, 190

multipoint conferences, H.323, 261

multisite WAN with centralized call processing deployment model, 40-43

multisite WAN with distributed call processing deployment model, 45-47

N

NANP (North American Numbering Plan), 321, 351

national numbering plans, 349

NFAS (Non-Facility Associated Signaling), 208

NM-HDV (High-Density Voice Network Module), DSP requirements, 98, 101-103

no such number tone, 140

NSE (Named Signaling Event), 75, 84

NTEs (Named Telephone Events), 83

NULL cipher, 20

num-exp command, 368

number expansion, 374-375
example, 376-377

number normalization, 355-356

numbering plans, 322, 349
example, 360
internal and public, integrating, 354
NANP, 351
number normalization, 355-356
overlapping, 352
private
designing, 349
integrating with public, 353
PSTN, 350
scalable, 351
VoIP, accomodating, 355-356

O

objectives of QoS, 64

off-net calls, 127

off-ramp faxing, 74

on-net calls, 126

on-net to off-net calls, 130-131

on-ramp faxing, 74

out-of-band DTMF support, 84

outbound ANI, configuring on T1 CAS trunks, 216-218
outbound dial peers, matching process, 179, 402
outbound PSTN calls, 329
outbound site code dialing, configuring, 415-416
outgoing call legs, 397
overlapping numbering plans, 352

P

packages, 279
- MGCP, 282

packet loss, 56, 60
PAMS (Perceptual Analysis Measurement System), 62
path replacement, 234
path selection, 322, 325, 397, 406
PBX-to-PBX calls, 128
PCM (pulse code modulation), 66
peer-to-peer signaling protocols, 8
PESQ (Perceptual Evaluation of Speech Quality), 62
physical E&M interface, 142
PLAR (Private Line Automatic Ringdown), 127, 147
PLC (Packet Loss Concealment), 60
POTS dial peers, 166
- configuring, 167-169
- digit manipulation, 375

PQ (priority queuing), 65
prefix command, 368
PRI interfaces, 193-194
PRI/BRI backhaul, 11
private numbering plans, 349
progress IE, 201
progress tones, 140
protocol interworking on Cisco UBE, 526
proxy servers, 294, 298
PSAP (Public Safety Answering Point), 357
PSQM (Perceptual Speech Quality Measurement), 61
PSTN, 321
- dial plans
  - *configuring, 331-340*
  - *inbound calls, 329*
  - *outbound calls, 329*
  - *requirements, 328*
  - *verifying, 341-348*
- numbering plans, 350

PSTN fallback, 64
public numbering plans, 349
PVDM2, DSP requirements, 98, 101, 103

Q

Q.850 cause codes, 342-344
Q.921 signaling, 195
Q.931 signaling, 195-198
QoS (quality of service), 63
QSIG, 23, 232
- configuring, 236
- features, 233-234
- over BRI, configuring, 238
- over PRI, configuring, 236-237
- path replacement, 234

R

R2 signaling, 187

RAI (Resource Availability Indicator), 510

configuring, 511-512

verifying operation, 512-515

RAS (registration, admission, and status), 10, 445

H.323 gatekeeper signaling, 446-450

Admission Request messages, 453-455

Blast LRQ messages, 459-460

call disconnect, 463

call flow, 464- 468

Gatekeeper Discovery messages, 450-451

Information Request messages, 455

interzone call setup, configuring, 462-463

intrazone call setup, configuring, 460

Location Request messages, 456

RRQ messages, 452-453

Sequential LRQ messages, 457

receiver off-hook tone, 140

redirect servers, 298

registrar servers, 298

regular expressions in translation rules, 382

remote failover, 48

reorder tone, 140

repacketization, 93

replay protection, 21

requirements for IP telephony gateways, 22

RGWs (residential gateways), 278

MGCP, configuring, 285-286

ring-back tone, 140

robbed-bit signaling, 188

RRQ (Registration Request) messages (RAS), 452-453

RSVP (Resource Reservation Protocol), 64

RSVP-based CAC on Cisco UBE, 530

RTP (Real-Time Transport Protocol), 16-17

RTPCP (RTP Control Protocol), 18

RTSP (Real-time Streaming Protocol), 17

S

scalable numbering plans, 351

SCCP (Skinny Client Control Protocol), 12-14

configuring, 109, 116-119

sccp ccm group command, 118

sccp ccm identifier command, 117

sccp command, 117

sccp local command, 117

search and replace opeations in translation rules, 384

Segmented Integer Counter Mode (AES), 20

selective routers, 358

Sequential LRQ messages (RAS), 457

show call active voice command, 229

show call history voice command, 230-232

show call resource voice threshold command, 512

show ccm-manager command, 291

show controller command, 239

show controller t1 command, 227
show dial-peer voice summary command, 341
show dialplan number commands, 341, 378-379
show dspfarm profile command, 119-120
show gatekeeper endpoint command, 515
show gatekeeper endpoints command, 487
show gateway command, 274, 514
show isdn status command, 239
show mgcp command, 290
show mgcp endpoint command, 292
show sip-ua calls command, 311
show voice call summary command, 228
show voice dsp command, 228
show voice port summary command, 226
side tone, 56
signaling, 7-9
CAS
E1 R2 CAS, 189
T1 CAS, 188
H.323, 9-10, 13
call flow, 464- 468
RAS signal messages, 446-463
MGCP, 13
PRI/BRI backhaul, 11
NFAS, 208
QSIG, 232
configuring, 236-238
features, 233-234
path replacement, 234
SCCP, 12-14
SIP, 14
single-site deployment model, 36-38
SIP (Session Initiation Protocol), 14, 298
addressing, 302-303
call flow, 299-302
configuring, 306-308
DTMF relay, 304-305
DTMF support, 83-84
T.38 fax relay, 79-80
verifying configuration, 309-314
site-code dialing, 406-408
configuring, 410-414
inbound, configuring, 416
outbound, configuring, 415-416
SMDI (Simplified Message Desk Interface), 22
software MTPs, 94
sound quality
MOS, 61
PESQ, 62
PSQM, 61
sound quality, factors affecting
packet loss, 60
delay, 57
jitter, 57
SRST (Survivable Remote Site Telephony), 328
COR, 426, 433-434
sRTCP (Secure RTCP), 20
SSDC5A signaling, 142
standalone voice gateways, 30
Cisco 827-4V ADSL router, 32
Cisco 7200 Series routers, 34
Cisco AS5300 Series Universal gateways, 31

Cisco AS5400 Series Universal gateways, 31
Cisco AS5850 Series Universal gateways, 31
Cisco ATA 186, 33
Cisco VG200 Series gateways, 30
station-id commands, 377
store-and-forward fax, 67, 73
super frames, 187
supervisory signaling, 135-138

T

T.38 fax relay, 66, 71, 77-80
T1 CAS trunks, 187-188
configuring, 208-218
T1 voice circuits, 185
TDM (time-division multiplexing), 188
technology prefixes, 444
configuring, 469-471, 495-497
TEHO (tail-end hop-off), 46, 407-409
configuring, 417-419
terminals (H.323), 254
TGW (terminating gateway), 74, 278
MGCP, configuring, 286
time slots, 190
timers, configuring on H.323 gateways, 267
timing parameters for voice ports, 159-160
toll-bypass, 406-408
configuring, 410-414
transcoders, 55, 92
configuring, 113
voice gateways, configuring, 107-109
translation rules, 380-382
configuring, 396-397
regular expressions, 382
search and replace operations, 384
verifying, 392-393
transparent codec pass-through, configuring on Cisco UBE, 543
troubleshooting MGCP, 293
trunks, 150, 134
analog, 152-154
CAMA, 154-157
DID, configuring, 157-159
intercluster trunk calls, 129-130
QSIG, verifying, 239-240, 242
Type I signaling, 141
Type II signaling, 141
Type III signaling, 141
Type IV signaling, 141
Type V signaling, 142

U-V

UAC (user agent client, 297
UAS (user agent server), 297
UBEs, 255-256
user agents, 294

VAD, effect on bandwidth, 90-91
verifying
COR, 434
digital voice ports, 225-232
DSP farm configuration, 119-120
gatekeepers, 487-488, 502-504
RAI, 512-515

H.323 gateway configuration, 274-275
MGCP configuration, 290-293
PSTN dial plans, 341-348
QSIG trunks, 239-242
SIP configuration, 309-314
translation rules, 392-393
voice port configuration, 160, 163
zone bandwidth operation, 509

via-zone gatekeepers, configuring on Cisco UBE, 544-548

voice band data, 66-69, 75

voice card command, 115

voice compression, codec complexity, 95-97

voice gateways. ***See*** **gateways**

voice ports, 132
analog, 133- 144
E&M voice ports, configuring, 148-150
FXO voice ports, configuring, 146-148
FXS voice ports, configuring, 144-146
timing parameters, 159-160
verifying configuration, 160, 163

voice samples, effect on bandwidth, 87-88

voice termination, 92

voice translation, 369, 380-381
profiles, 385-386
and dialplan-pattern command, 390-392
processing order, 386-389
rules, 382
regular expressions, 382
search and replace operations, 384
verifying, 392-393

voice-class codec command, 265

voice-translation profiles, 380

VoIP, 4
adding to numbering plan, 355-356
business case for, 4-6
dial peers, 166
configuring, 169-172
fax transmissions, 66
Cisco Fax Relay, 76-77
fax pass-through, 67-69
fax relay, 69
H.323 T.38 fax relay, 77-79
MGCP T.38 fax relay, 80
modem pass-through, 69
SIP T.38 fax relay, 79-80
store-and-forward fax, 73
gateways, 21-23
media transmission protocols, 16
modem relay, 71-73
network components, 7
required functionality, 7-9
service considerations, 15
signaling protocols
H.323, 9-10, 13
MGCP, 11-13
SCCP, 12-14
SIP, 14

W-X-Y-Z

when to use cRTP, 20
white noise, 91
wink-start signaling, 143

XGCP (External Gateway Control Protocol), 80

zone bandwidth, verifying, 509
zone prefixes, 444
configuring, 468-469, 494
zones, 444
configuring, 493