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, CCIE No. 7945

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

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.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:
U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States lease contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Cisco Press Program Manager: Jeff Brady

Executive Editor: Brett Bartow

Managing Editor: Patrick Kanouse

Development Editor: Andrew Cupp

Senior Project Editor: San Dee Phillips

Copy Editor: Barbara Hacha

Technical Editors: Michelle Plumb
Anthony Sequeira

Editorial Assistant: Vanessa Evans

Book and Cover Designer: Louisa Adair

Composition: Bronkella Publishing, LLC

Indexer: Tim Wright

Proofreader: Jovana San Nicholas-Shirley

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

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

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

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

About the Author

Kevin Wallace, CCIE No. 7945, is a certified Cisco instructor, and he teaches courses in the Cisco CCSP, CCVP, and CCNP tracks. With 19 years of Cisco networking experience, Kevin has been a network design specialist for the Walt Disney World Resort and a network manager for Eastern Kentucky University. Kevin holds a bachelor of science degree in electrical engineering from the University of Kentucky. Kevin also is a CCVP, CCSP, CCNP, and CCDP with multiple Cisco security and IP communications specializations.

About the Technical Reviewers

Michelle Plumb is a full-time certified Cisco instructor for SkillSoft, focusing on the Cisco IP Telephony track. Michelle has more than 18 years in the field as an IT and telephony specialist and maintains a high level of Cisco and Microsoft certifications, including CCVP, CCSI, and MCSE NT 4.0/2000. Michelle has been a technical reviewer for numerous books related to the Cisco CCNP and Cisco IP Telephony course material track.

Anthony Sequeira, CCIE No. 15626, completed the CCIE in Routing and Switching in January 2006. He is currently pursuing the CCIE in Security. For the past 15 years, he has written and lectured to massive audiences about the latest in networking technologies. Anthony is currently a senior technical instructor and certified Cisco instructor for SkillSoft. Anthony lives with his wife and daughter in Florida. When he is not reading about the latest Cisco innovations, he is exploring the Florida skies in a Cessna.

Dedication

I dedicate this book to my two daughters, Stacie and Sabrina. You are growing up far too fast.

Acknowledgments

My thanks go out to my fellow instructors at SkillSoft and our manager, Tom Warrick. It is an honor to work side by side with you all. Also, thanks to Brett Bartow at Cisco Press for his faith in me and allowing me to simultaneously author two books.

On a personal note, I acknowledge and thank God for His blessings in my life. Also, my wife, Vivian, and my daughters, Stacie and Sabrina, have patiently awaited the completion of this book and the *CCNA Security Official Exam Certification Guide*. Thank you for your patience during these past few months.

This Book Is Safari Enabled

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

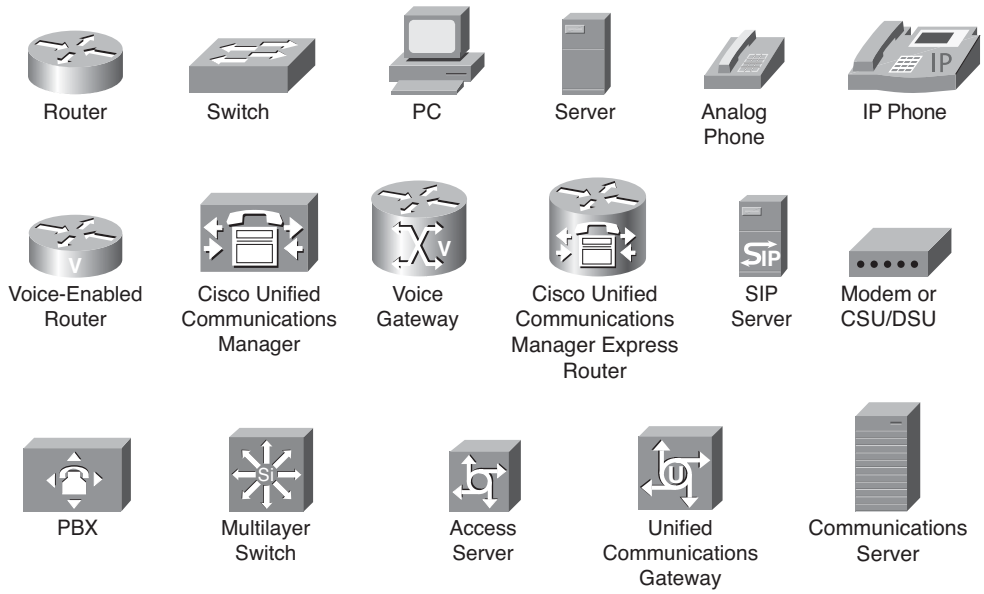
- Go to http://www.informit.com/onlineedition.
- Complete the brief registration form.
- Enter the coupon code 89GJ-11QH-EDPS-48IP-AJ6C.

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

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 Voice over IP (VoIP), components of a VoIP network, the protocols used, and service considerations of integrating VoIP into an existing data network.
- Describe various types of voice gateways and how to use gateways in different IP telephony environments.

CHAPTER 1

Introducing Voice over IP Networks

Voice over Internet Protocol (VoIP) allows a voice-enabled router to carry voice traffic, such as telephone calls and faxes, over an Internet Protocol (IP) network. This chapter introduces the fundamentals of VoIP, the various types of voice gateways, and how to use gateways in different IP telephony environments.

VoIP Fundamentals

Voice over IP is also known as VoIP. You might also hear VoIP referred to as *IP Telephony*. Both terms refer to sending voice across an IP network. However, the primary distinction revolves around the endpoints in use. For example, in a VoIP network, traditional analog or digital circuits connect into an IP network, typically through some sort of gateway. However, an IP telephony environment contains endpoints that natively communicate using IP. Be aware that much of the literature on the subject, including this book, might use these terms interchangeably.

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

Cisco Unified Communications Architecture

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

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

- **IP telephony:** IP telephony refers to technology that transmits voice communications over a network using IP standards. Cisco Unified Communications System includes hardware and software products such as call processing agents, IP phones (both wired and wireless), voice messaging systems, video devices, and other special applications.
- **Customer contact center:** Cisco IP Contact Center products combine strategy with architecture to enable efficient and effective customer communications across a global network. This allows organizations to draw from a broader range of resources to service customers. These resources include access to a large pool of customer service agents and multiple channels of communication as well as customer self-help tools.
- **Video telephony:** The Cisco Unified Video Advantage products enable real-time video communications and collaboration using the same IP network and call processing agent as Cisco Unified Communications. With Cisco Unified Video Advantage, making a video call is just as easy as dialing a phone number.
- **Rich-media conferencing:** Cisco Conference Connection and Cisco Unified MeetingPlace enhance the virtual meeting environment with an integrated set of IP-based tools for voice, video, and web conferencing.
- **Third-party applications:** Cisco works with other companies to provide a selection of third-party IP communications applications and products. This helps businesses focus on critical needs such as messaging, customer care, and workforce optimization.

VoIP Overview

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

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

Business Case for VoIP

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

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

- **Cost savings:** Traditional time-division multiplexing (TDM), which is used in the public switched telephone network (PSTN) environment, dedicates 64 kbps of bandwidth per voice channel. This approach results in bandwidth being unused when no voice traffic exists. VoIP shares bandwidth across multiple logical connections, which results in a more efficient use of the bandwidth, thereby reducing bandwidth requirements. A substantial amount of equipment is needed to combine 64-kbps channels into high-speed links for transport across a network. Packet telephony uses statistical analysis to multiplex voice traffic alongside data traffic. This consolidation results in substantial savings on capital equipment and operations costs.
- **Flexibility:** The sophisticated functionality of IP networks allows organizations to be flexible in the types of applications and services they provide to their customers and users. Service providers can easily segment customers. This helps them to provide different applications, custom services, and rates depending on traffic volume needs and other customer-specific factors.
- **Advanced features:** Following are some examples of the advanced features provided by current VoIP applications:
  - **Advanced call routing:** When multiple paths exist to connect a call to its destination, some of these paths might be preferred over others based on cost, distance, quality, partner handoffs, traffic load, or various other considerations. Least-cost routing and time-of-day routing are two examples of advanced call routing that can be implemented to determine the best possible route for each call.
  - **Unified messaging:** Unified messaging improves communications and productivity. It provides a single user interface for messages that have been delivered over a variety of mediums. For example, users can read their e-mail, hear their voice mail, and view fax messages by accessing a single inbox.
  - **Integrated information systems:** Organizations use VoIP to affect business process transformation. These processes include centralized call control, geographically dispersed virtual contact centers, and access to resources and self-help tools.
  - **Long-distance toll bypass:** Long-distance toll bypass is an attractive solution for organizations that place a significant number of calls between sites that are charged traditional long-distance fees. In this case, it might be more cost-effective to use VoIP to place those calls across an IP network. If the IP WAN becomes congested, calls can overflow into the PSTN, ensuring that no degradation occurs in voice quality.

- **Security:** Mechanisms in an IP network allow an administrator to ensure that IP conversations are secure. Encryption of sensitive signaling header fields and message bodies protect packets in case of unauthorized packet interception.
- **Customer relationships:** The capability to provide customer support through multiple mediums, such as telephone, chat, and e-mail, builds solid customer satisfaction and loyalty. A pervasive IP network allows organizations to provide contact center agents with consolidated and up-to-date customer records along with related customer communication. Access to this information allows quick problem solving, which builds strong customer relationships.
- **Telephony application services:** XML services on Cisco IP Phones give users another way to perform or access business applications. Some examples of XML-based services on Cisco IP Phones are user stock quotes, inventory checks, direct-dial directory, announcements, and advertisements. Some Cisco IP Phones are equipped with a pixel-based display that can display full graphics instead of just text in the window. The pixel-based display capabilities allow you to use sophisticated graphical presentations for applications on Cisco IP Phones and make them available at any desktop, counter, or location.

Components of a VoIP Network

Figure 1-1 depicts the basic components of a packet voice network.

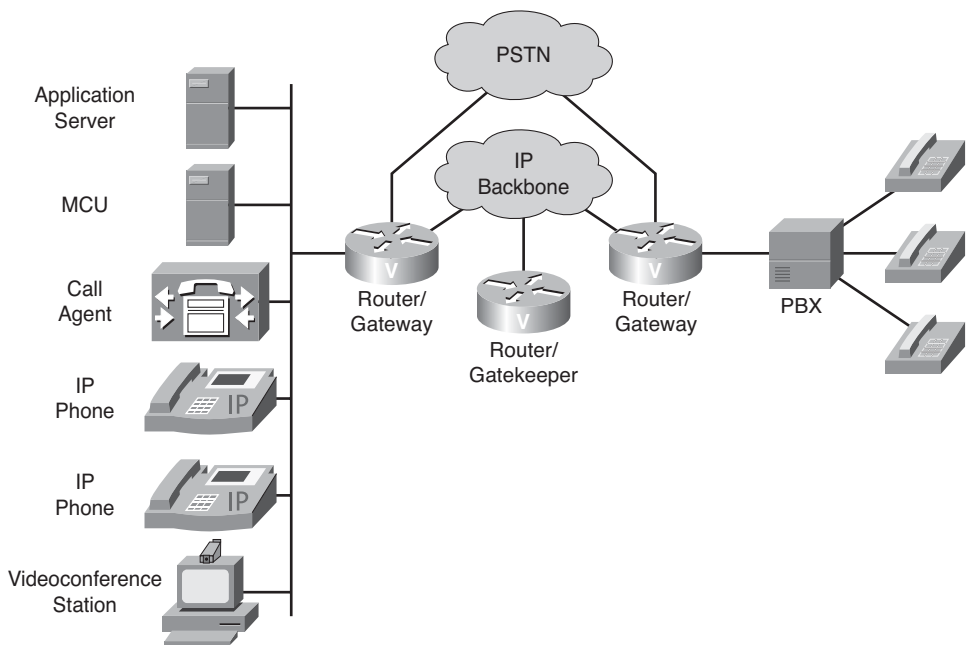


Figure 1-1 *Components of a VoIP Network*

The following is a description of these basic components:

- **IP Phones:** Cisco IP Phones provide IP endpoints for voice communication.
- **Gatekeeper:** A gatekeeper provides Call Admission Control (CAC), bandwidth control and management, and address translation.
- **Gateway:** The gateway provides translation between VoIP and non-VoIP networks, such as the PSTN. Gateways also provide physical access for local analog and digital voice devices, such as telephones, fax machines, key sets, and private branch exchanges (PBX).
- **Multipoint Control Unit (MCU):** An MCU provides real-time connectivity for participants in multiple locations to attend the same videoconference or meeting.
- **Call agent:** A call agent provides call control for IP phones, CAC, bandwidth control and management, and address translation. Unlike a gatekeeper, which in a Cisco environment typically runs on a router, a call agent typically runs on a server platform. Cisco Unified Communications Manager is an example of a call agent.
- **Application servers:** Application servers provide services such as voice mail, unified messaging, and Cisco Communications Manager Attendant Console.
- **Videoconference station:** A videoconference station provides access for end-user participation in videoconferencing. The videoconference station contains a video capture device for video input and a microphone for audio input. A user can view video streams and hear audio that originates at a remote user station.

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

VoIP Functions

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

Required VoIP functionality includes these functions:

- **Signaling:** Signaling is the capability to generate and exchange control information that will be used to establish, monitor, and release connections between two endpoints. Voice signaling requires the capability to provide supervisory, address, and alerting functionality between nodes. The PSTN network uses Signaling System 7 (SS7) to transport control messages. SS7 uses out-of-band signaling, which, in this case, is the exchange of call control information in a separate dedicated channel.

VoIP presents several options for signaling, including H.323, Session Initiation Protocol (SIP), H.248, Media Gateway Control Protocol (MGCP), and Skinny Client Control Protocol (SCCP). Some VoIP gateways are also capable of initiating SS7 signaling directly to the PSTN network. Signaling protocols are classified as either peer-to-peer or client/server protocols.

SIP and H.323 are examples of peer-to-peer signaling protocols where the end devices or gateways contain the intelligence to initiate and terminate calls and interpret call control messages. H.248, SCCP, and MGCP are examples of client/server protocols where the endpoints or gateways do not contain call control intelligence but send or receive event notifications to a server commonly referred to as a *call agent*. For example, when an MGCP gateway detects a telephone that has gone off hook, it does not know to automatically provide a dial tone. The gateway sends an event notification to the call agent, telling the agent that an off-hook condition has been detected. The call agent notifies the gateway to provide a dial tone.

- **Database services:** Access to services, such as toll-free numbers or caller ID, requires the capability to query a database to determine whether the call can be placed or information can be made available. Database services include access to billing information, caller name delivery (CNAM), toll-free database services, and calling-card services. VoIP service providers can differentiate their services by providing access to many unique database services. For example, to simplify fax access to mobile users, a provider can build a service that converts fax to e-mail. Another example is providing a call notification service that places outbound calls with prerecorded messages at specific times to notify users of such events as school closures, wake-up calls, or appointments.

- **Bearer control:** Bearer channels are the channels that carry voice calls. Proper supervision of these channels requires that appropriate call connect and call disconnect signaling be passed between end devices. Correct signaling ensures that the channel is allocated to the current voice call and that a channel is properly deallocated when either side terminates the call. Connect and disconnect messages are carried by SS7 in the PSTN network. Connect and disconnect message are carried by SIP, H.323, H.248, or MGCP within the IP network.

- **Codecs:** Codecs provide the coding and decoding translation between analog and digital facilities. Each codec type defines the method of voice coding and the compression mechanism that is used to convert the voice stream. The PSTN uses TDM to carry each voice call. Each voice channel reserves 64 kbps of bandwidth and uses the G.711 codec to convert an analog voice wave to a 64-kbps digitized voice stream. In VoIP design, codecs might compress voice beyond the 64-kbps voice stream to allow more efficient use of network resources. The most widely used codec in the WAN environment is G.729, which compresses the voice stream to 8 kbps.

VoIP Signaling Protocols

VoIP uses several control and call-signaling protocols. Among these are:

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

The H.323 Umbrella

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

The protocols specified by H.323 include the following:

- **H.225 Call Signaling:** H.225 call signaling is used to establish a connection between two H.323 endpoints. This is achieved by exchanging H.225 protocol messages on the call-signaling channel. The call-signaling channel is opened between two H.323 endpoints or between an endpoint and an H.323 gatekeeper.
- **H.225 Registration, Admission, and Status:** Registration, admission, and status (RAS) is the protocol between endpoints (terminals and gateways) and gatekeepers. RAS is used to perform registration, admission control, bandwidth changes, status, and disengage procedures between endpoints and gatekeepers. A *RAS channel* is used to exchange RAS messages. This signaling channel is opened between an endpoint and a gatekeeper prior to the establishment of any other channels.
- **H.245 Control Signaling:** H.245 control signaling is used to exchange end-to-end control messages governing the operation of an H.323 endpoint. These control messages carry information related to the following:
  - Capabilities exchange
  - Opening and closing of logical channels used to carry media streams
  - Flow-control messages
  - General commands and indications
- **Audio codecs:** An audio codec encodes the audio signal from a microphone for transmission by the transmitting H.323 terminal and decodes the received audio code that is sent to the speaker on the receiving H.323 terminal. Because audio is the minimum service provided by the H.323 standard, all H.323 terminals must have at least one audio codec supported, as specified in the ITU–T G.711 recommendation (coding audio at 64 kbps). Additional audio codec recommendations such as G.722 (64, 56, and 48 kbps), G.723.1 (5.3 and 6.3 kbps), G.728 (16 kbps), and G.729 (8 kbps) might also be supported.
- **Video codecs:** A video codec encodes video from a camera for transmission by the transmitting H.323 terminal and decodes the received video code on a video display of the receiving H.323 terminal. Because H.323 specifies support of video as optional, the support of video codecs is optional as well. However, any H.323 terminal providing video communications must support video encoding and decoding as specified in the ITU–T H.261 recommendation.

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

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

MGCP

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

MGCP is a plain-text protocol used by call-control devices to manage IP telephony gateways. MGCP was defined under RFC 2705, which was updated by RFC 3660, and superseded by RFC 3435, which was updated by RFC 3661.

With MGCP, Cisco UCM knows of and controls individual voice ports on an MGCP gateway. This approach allows complete control of a dial plan from Cisco UCM and gives Communications Manager per-port control of connections to the PSTN, legacy PBX, voice-mail systems, and POTS phones. MGCP is implemented with use of a series of plain-text commands sent via User Datagram Protocol (UDP) port 2427 between the Cisco UCM and a gateway.

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

PRI/BRI Backhaul

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

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

Session Initiation Protocol

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

SIP is a peer-to-peer protocol where user agents (UAs) initiate sessions, similar to H.323. However, unlike H.323, SIP uses ASCII-text-based messages to communicate. Therefore, you can implement and troubleshoot SIP very easily.

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

Skinny Client Control Protocol

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

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

Comparing VoIP Signaling Protocols

The primary goal for all four of the previously mentioned VoIP signaling protocols is the same—to create a bidirectional Real-time Transport Protocol (RTP) stream between VoIP endpoints involved in a conversation. However, VoIP signaling protocols use different architectures and procedures to achieve this goal.

H.323

H.323 is considered a peer-to-peer protocol, although H.323 is not a single protocol. Rather, it is a suite of protocols. The necessary gateway configuration is relatively complex, because you need to define the dial plan and route patterns directly on the gateway. Examples of H.323-capable devices are the Cisco VG224 Analog Phone Gateway and the Cisco 2600XM Series, Cisco 2800 Series, 3700 Series, and 3800 Series routers.

The H.323 protocol is responsible for all the signaling between a Cisco UCM cluster and an H.323 gateway. The ISDN protocols, Q.921 and Q.931, are used only on the Integrated Services Digital Network (ISDN) link to the PSTN, as illustrated in Figure 1-2.

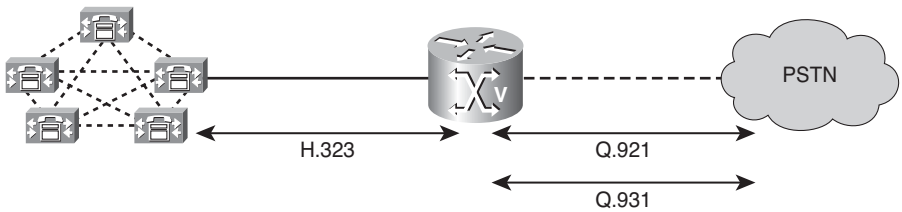


Figure 1-2 *H.323 Signaling*

MGCP

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

MGCP is used to manage a gateway. All ISDN Layer 3 information is backhauled to a Cisco UCM server. Only the ISDN Layer 2 information (Q.921) is terminated on the gateway, as depicted in Figure 1-3.

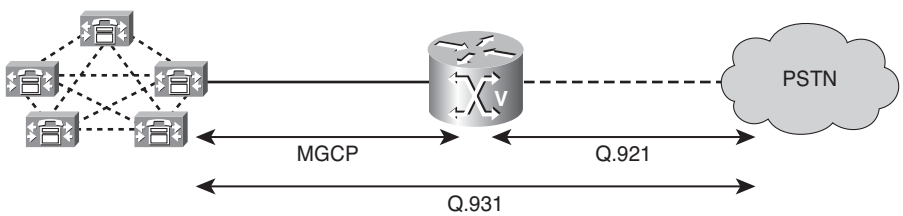


Figure 1-3 *MGCP Signaling*

SIP

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

The SIP protocol is responsible for all the signaling between a Cisco UCM cluster and a gateway. The ISDN protocols, Q.921 and Q.931, are used only on an ISDN link to the PSTN, as illustrated in Figure 1-4.

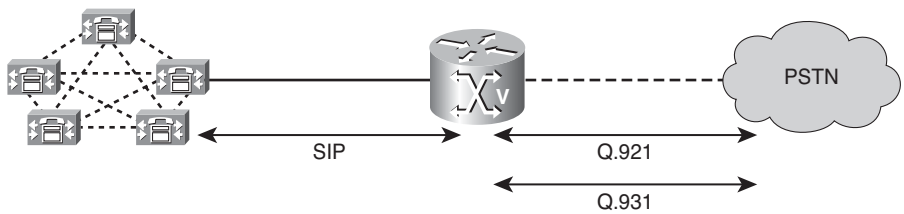


Figure 1-4 *SIP Signaling*

SCCP

SCCP works in a client/server architecture, as shown in Figure 1-5, which simplifies the configuration of SCCP devices such as Cisco IP Phones and Cisco ATA 180 Series and VG200 Series FXS gateways.

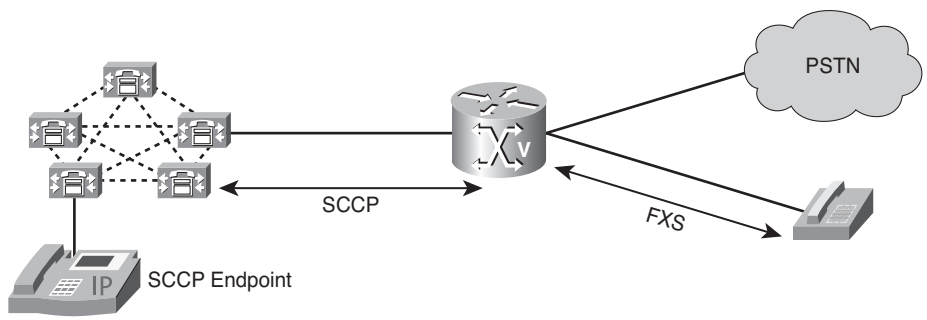


Figure 1-5 *SCCP Signaling*

SCCP is used on Cisco VG224 and VG248 analog phone gateways. ATAs enable communications between Cisco UCM and a gateway. The gateway then uses standard analog signaling to an analog device connected to the ATA's FXS port. Recent versions of Cisco IOS voice gateways—for example, the 2800 series—also support SCCP controlled Foreign Exchange Station (FXS) ports.

VoIP Service Considerations

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

Table 1-1 lists issues associated with implementing VoIP in a converged network and solutions that address these issues.

Table 1-1 *Issues and Solutions for VoIP in a Converged Network*

Issue	Solutions
Latency	Increase bandwidth. Choose a different codec type. Fragment data packets. Prioritize voice packets.
Jitter	Use dejitter buffers. Prioritize voice packets.
Bandwidth	Calculate bandwidth requirements, including voice payload, overhead, and data.
Packet loss	Design the network to minimize congestion. Prioritize voice packets. Use codecs to minimize small amounts of packet loss.
Reliability	Provide redundancy for hardware, links, and power (uninterruptible power supply [UPS]). Perform proactive network management.
Security	Secure the following components: ■ Network infrastructure ■ Call-processing systems ■ Endpoints ■ Applications

Media Transmission Protocols

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

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

Real-Time Transport Protocol

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

RTP provides end-to-end network transport functions intended for applications with real-time transmission requirements, such as audio and video. Those functions include payload-type identification, sequence numbering, time stamping, and delivery monitoring. Figure 1-6 shows a typical role played by RTP in a VoIP network. Specifically, notice RTP communicates directly between the voice endpoints, whereas the call setup protocols (that is, H.225 and H.245 in this example) are used to communicate with voice gateways.

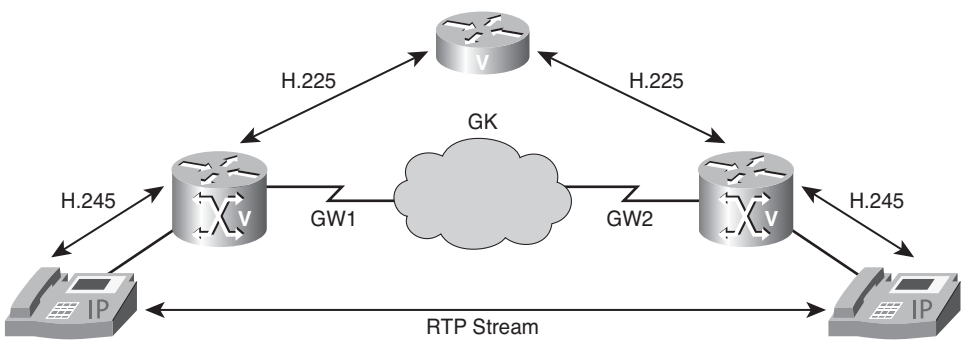


Figure 1-6 *Role of RTP*

RTP typically runs on top of UDP to use the multiplexing and checksum services of that protocol. RTP does not have a standard TCP or UDP port on which it communicates. The only standard it obeys is that UDP communications are done via an even port, and the next higher odd port is used for RTCP communications. Although no standards are assigned, in a Cisco environment RTP is generally configured to use UDP ports in the range 16,384–32,767.

RTP can carry any data with real-time characteristics, such as interactive audio or video. The fact that RTP uses a dynamic port range can make it difficult for it to traverse firewalls.

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

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

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

RTP Control Protocol

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

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

There are several types of RTCP packets: Sender Report Packet, Receiver Report Packet, Source Description RTCP Packet, Goodbye RTCP Packet, and application-specific RTCP packets.

RTCP provides the following feedback on current network conditions:

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

Compressed RTP

RTP includes a data portion and a header portion. The data portion of RTP is a thin protocol that provides support for the real-time properties of applications, such as continuous media, including timing reconstruction, loss detection, and content identification. The header portion of RTP is considerably larger than the data portion. The header portion consists of the IP segment, the UDP segment, and the RTP segment. Given the size of the IP/UDP/RTP segment combinations, it is inefficient to send the IP/UDP/RTP header without compressing it. Figure 1-7 illustrates using RTP header cRTP over a relatively low-speed WAN link (such as a T1 link), which could benefit from the bandwidth freed up by compressing the IP/UDP/RTP header.

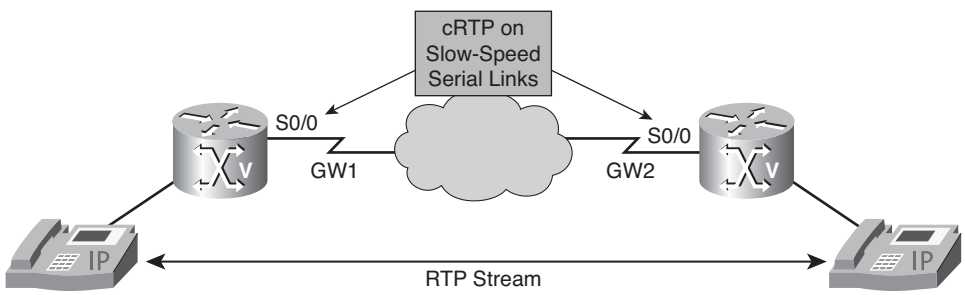


Figure 1-7 *RTP Header Compression*

The IP header portion consists of an IP segment, a UDP segment, and an RTP segment. The minimal 20 bytes of the IP segment, combined with the 8 bytes of the UDP segment and the 12 bytes of the RTP segment, create a 40-byte IP/UDP/RTP header. The RTP

packet has a payload of approximately 20 to 150 bytes for audio applications that use compressed payloads.

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

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

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

RFC 2509 was designed to work with reliable and fast point-to-point links. In less than optimal circumstances, where there might be long delays, packet loss, and out-of-sequence packets, cRTP doesn't function well for VoIP applications. Another adaptation, ECRPT, was defined in a subsequent Internet draft document to overcome that problem.

RTP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. It is also supported over ISDN interfaces.

Why and When to Use cRTP

cRTP does not technically perform compression. Rather, cRTP leverages the fact that much of the header information in every packet in a VoIP stream contains redundant information, and cRTP then suppresses the sending of that redundant information. For example, after a VoIP call flow is established, every packet has the same source and destination IP addresses, the same source and destination UDP port numbers, and the same RTP payload type. By caching this redundant information in the gateways at each end of a link, sending reduced headers, and then reassembling the full header, cRTP can achieve significant bandwidth savings without any loss of information.

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

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

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

Secure RTP

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

sRTP also has a sister protocol, called Secure RTCP (sRTCP). sRTCP provides the same security-related features to RTCP as the ones provided by sRTP to RTP. sRTP can be used in conjunction with compressed RTP. Figure 1-8 demonstrates that an sRTP flow travels between devices (Cisco IP phones in Figure 1-8), which are capable of sending and receiving sRTP traffic.

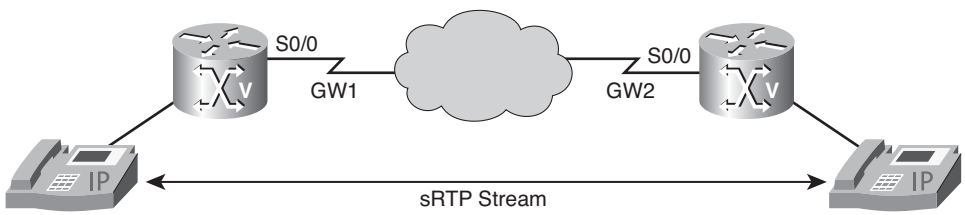


Figure 1-8 *Secure RTP Traffic Flow*

Flow Encryption

sRTP standardizes utilization of only a single cipher, Advanced Encryption Standard (AES), which can be used in two cipher modes, which turn the original block AES cipher into a stream cipher:

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

In addition to the AES cipher, sRTP gives the user the ability to disable encryption outright, using the so called NULL cipher. However, the NULL cipher does not perform any encryption. Rather, the encryption algorithm functions as though the key stream contains only zeroes, and it copies the input stream to the output stream without any changes.

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

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

Authentication and Integrity

The HMAC-SHA1 algorithm (defined in RFC 2104) is used to authenticate a message and protect its integrity. This algorithm produces a 160-bit result, which is then truncated to 80 bits to become the authentication tag, which is then appended to a packet. The HMAC is calculated over the packet payload and material from the packet header, including the packet sequence number.

Replay Protection

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

Introducing VoIP Gateways

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

Understanding Gateways

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

Following are the two types of Cisco access gateways:

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

IP telephony gateways should meet these core feature requirements:

- **Gateway protocol support:** Cisco voice gateways support various signaling protocols, depending on the hardware platform. Cisco gateways support H.323, MGCP, SIP, and SCCP. H.323 and SIP gateways do not need a call control agent. Therefore, they can be deployed on networks in which call agents, such as Cisco UCM, are not present. MGCP and SCCP are streamlined protocols that work only on a network in which a call agent, such as Cisco UCM, is present. Cisco IP Phones use SCCP, which is a lighter-weight protocol. SCCP uses a client-server model, whereas H.323 is a peer-to-peer model. MGCP also follows a client-server model.

Note Protocol selection depends on site-specific requirements and the installed base of equipment. For example, many remote branch locations have Cisco 2600XM Series or 3700 Series multiservice routers installed. These routers support H.323 and MGCP 0.1, beginning with Cisco IOS Release 12.2(11)T and Cisco UCM Release 3.1 or later. You might prefer MGCP to H.323 because of simpler configuration. This option also works well with older IOS versions because of support for call survivability during a Cisco UCM failover from a primary to a secondary Cisco UCM server. On the other hand, you might prefer H.323 over MGCP because of the wider selection of interfaces supported.

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

- **Advanced gateway functionality:** The gateways should support the ability to transmit, without corruption, touch-tone digits (that is, Dual Tone Multifrequency [DTMF] tones) and also support a collection of other user services, as follows:
  - **DTMF relay capabilities:** Each digit dialed with tone dialing is assigned a unique pair of frequencies. Voice compression of these tones with a low bit-rate codec can cause DTMF signal loss or distortion. Therefore, DTMF tones can be separated from the voice bearer stream and sent as signaling indications through the gateway protocol (H.323, SCCP, or MGCP) signaling channel instead.
  - **Supplementary services support:** These services provide user functions such as hold, transfer, and conferencing, and are considered to be fundamental requirements of any voice installation.
- **Work with redundant Cisco UCM:** The gateways must support the capability to "rehome" to a secondary Cisco UCM in the event of a primary Cisco UCM failure.
- **Call survivability in Cisco UCM:** The voice gateway preserves the RTP bearer stream (the voice conversation) between two IP endpoints when a Cisco UCM server to which an endpoint is registered is no longer accessible.
- **Q Signaling (QSIG) support:** QSIG is becoming the standard for PBX interoperability in Europe and North America. With QSIG, the Cisco voice packet network appears to PBXs as a distributed transit PBX that can establish calls to any PBX or other telephony endpoint served by a Cisco gateway, including non-QSIG endpoints.
- **Fax and modem support:** Fax over IP enables interoperability of traditional analog fax machines with IP telephony networks. The fax image is converted from an analog signal and is transmitted as digital data over a packet network.

Gateways are deployed usually as edge devices on a network. Because gateways might interface with both the PSTN and a company WAN, they must have appropriate hardware and utilize an appropriate protocol for that network. Figure 1-9 represents a scenario where three types of gateways are deployed for VoIP and PSTN interconnections.

The scenario shown in Figure 1-9 displays the unified communications network of a company that was recently formed as a result of a merger of three individual companies. In the past, each company had its own strategy in terms of how it connected to the PSTN:

- The San Jose location used a Cisco UCM environment with a MGCP-controlled unified communications gateway to connect to the PSTN.
- The Chicago location used a Cisco UCM Express environment with an H.323-based unified communications gateway to connect to the PSTN.

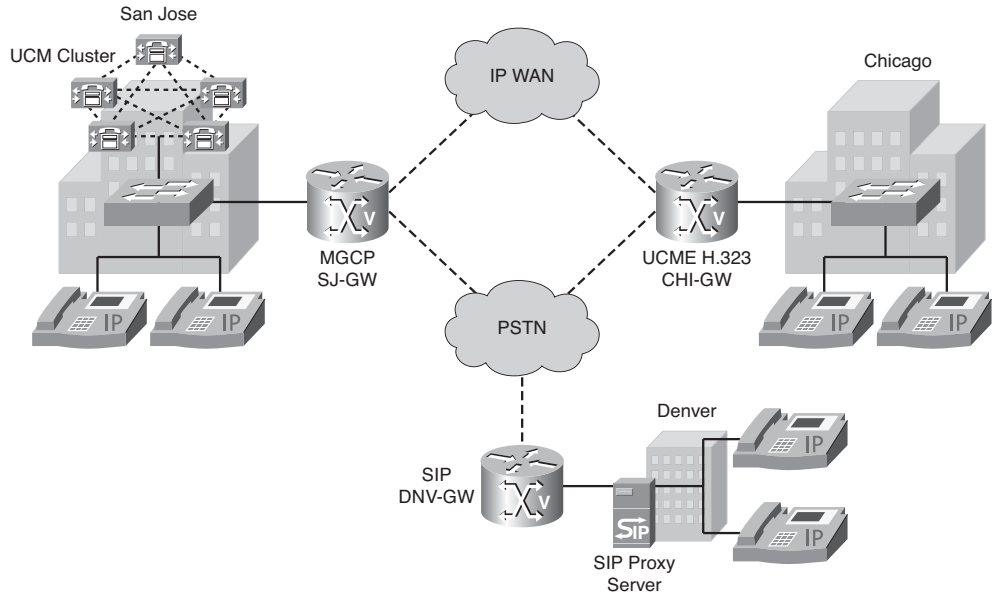


Figure 1-9 *Gateway Deployment Example*

- The Denver location used a Cisco SIP proxy server and SIP IP phones as well as a SIP-based unified communications gateway to connect to the PSTN. Because the Denver location is only a small office, it does not use the WAN for IP telephony traffic to the other locations. Therefore, Denver's local VoIP network is connected only to the PSTN.

Modern Gateway Hardware Platforms

This section covers some of the current Cisco voice gateway models used in today's enterprise environments.

Cisco 2800 Series Integrated Services Routers

The Cisco 2800 Series Integrated Services Routers, as pictured in Figure 1-10, comprise four models (listed from top to bottom): Cisco 2801, Cisco 2811, Cisco 2821, and Cisco 2851. The 2800 Series provides increased security, voice, and overall performance, embedded service options, and dramatically increased slot performance and density, as compared to older 2600 Series models. It also maintains support for most of the more-than-90 modules available for the Cisco 1700 Series Modular Access Routers, 2600 Series Multiservice Platforms, and 3700 Series Multiservice Access Routers.

Figure 1-10 *Cisco 2800 Series Integrated Services Routers*

The 2800 Series can deliver simultaneous, high-quality, wire-speed services up to multiple T1/E1/xDSL connections. The routers offer embedded encryption acceleration and, on the motherboard, voice digital-signal-processor (DSP) slots. They also offer intrusion prevention system (IPS) and firewall functions, optional integrated call processing and voice-mail support, high-density interfaces for a wide range of wired and wireless connectivity requirements, and sufficient performance and slot density for future network expansion requirements and advanced applications. Go to http://www.cisco.com/go/2800 to learn more about the Cisco 2800 Series routers.

Cisco 3800 Series Integrated Services Routers

The Cisco 3800 Series Integrated Services Routers, as shown in Figure 1-11, also feature embedded security processing, significant performance and memory enhancements, and new high-density interfaces that deliver the performance, availability, and reliability required to scale mission-critical security, IP telephony, business video, network analysis, and web applications in today's enterprise environments. The 3800 Series routers deliver multiple concurrent services at wire-speed T3/E3 rates.

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

Figure 1-11 *Cisco 3800 Series Integrated Services Routers*

New 3800 Series models include the Cisco 3825 Integrated Services Router and the Cisco 3845 Integrated Services Router, available with three optional configurations for AC power, AC power with integrated inline power support, and DC power. Go to http://www.cisco.com/go/3800 to learn more about the 3800 Series routers.

Cisco Catalyst 6500 Series Switches

The Cisco Catalyst 6500 Series Switches, as shown in Figure 1-12, are high-performance and feature-rich platforms that can be used as voice gateways by installing a Cisco Communication Media Module (CMM).

Figure 1-12 *Cisco Catalyst 6500 Series Switches*

The CMM is a Cisco Catalyst 6500 Series line card that provides flexible and high-density VoIP gateway and media services. A Catalyst 6500 Series Switch can handle multiple digital trunk interfaces. For example, the Cisco Catalyst 6509 Switch supports up to 144 T1/E1 connections by using eight communications media modules with 18 ports each. These gateway and media services allow organizations to connect their existing TDM network to their IP communications network, provide connectivity to the PSTN, and enable conferencing and transcoding services. Go to http://www.cisco.com/go/catalyst6500 to learn more about the Catalyst 6500 Series Switches.

Well-Known and Widely Used Enterprise Models

Several Cisco modular access routers that might already be installed in enterprise networks have voice gateway capabilities. Although some of these models are well known and widely used, they have reached end of sale (EOS) status. However, because these routers were the leading voice gateway products for a long time, you should be familiar with and know how to support these models.

Cisco 1751-V Modular Access Router

The Cisco 1751-V modular access router, as pictured in Figure 1-13, supports multiservice integration of voice, video, data, and fax traffic. The router offers many WAN-access and voice-interface options, VoIP, high-performance routing with bandwidth management, inter-VLAN routing, and virtual private network (VPN) access with a firewall. Go to http://www.cisco.com/go/1700 to learn more about the Cisco 1700 Series Modular Access Routers.

Figure 1-13 *Cisco 1751-V*

Cisco 1760-V Modular Access Router

The Cisco 1760-V Modular Access Router, as depicted in Figure 1-14, offers small-to-medium-sized businesses and small-enterprise branch offices a 19-inch rack-mount access solution designed to take advantage of the productivity of business applications. The router ensures the multiservice integration of voice, video, data, and fax traffic. It provides businesses with the complete functionality and flexibility to deliver secure Internet

and intranet access. The router has many WAN access options, VoIP, high-performance routing with QoS, inter-VLAN routing, and VPN access with firewall options.

Figure 1-14 *Cisco 1760-V*

Cisco 2600XM Series Multiservice Routers

The modular architecture of the Cisco 2600XM Series multiservice routers, as shown in Figure 1-15, enables you to upgrade interfaces to accommodate network expansion or changes in technology as new services and applications are deployed. Modular interfaces are shared with the Cisco 1700 Series Modular Access Routers and the Cisco 3700 Series Multiservice Access Routers, providing investment protection and reducing the complexity of managing a remote network solution by integrating the functions of multiple, separate devices into a single, compact unit. Network modules available for the 2600XM Series and 3700 Series support many applications, including multiservice voice and data integration, integrated switching, analog and ISDN dial access, and serial device concentration. Go to http://www.cisco.com/go/2600 to learn more about the Cisco 2600XM Series multiservice routers.

Figure 1-15 *Cisco 2600XM Series*

Cisco 3600 Series Multiservice Access Routers

The Cisco 3600 Series, as shown in Figure 1-16, is a family of modular, multiservice access platforms for medium- and large-sized offices and smaller Internet service providers (ISPs). With more than 70 modular interface options, the Cisco 3600 Series provides solutions for data, voice, video, hybrid dial access, VPNs, and multiprotocol data routing. The high-performance, modular architecture protects customers' investments in network technology and integrates the functions of several devices within a single, manageable solution.

Figure 1-16 *Cisco 3600 Series*

Cisco extended the Cisco 3600 Series with the Cisco 3660 multiservice access platform. The Cisco 3660 platform provides higher densities, greater performance, and more expansion capabilities. The additional power and performance of the Cisco 3660 platform enables new applications, such as packetized voice aggregation and branch office Asynchronous Transfer Mode (ATM) access ranging from T1/E1 inverse multiplexing over ATM (IMA) to Optical Carrier 3 (OC-3). Go to http://www.cisco.com/go/3600 to learn more about the Cisco 3600 Series multiservice access routers.

Cisco 3700 Series Multiservice Access Routers

The Cisco 3700 Series Multiservice Access Routers, as illustrated in Figure 1-17, are modular routers that enable flexible and scalable deployment of e-business applications for the Cisco Full Service Branch (FSB) office. The 3700 Series Multiservice Access Routers optimize the branch office with high-performance routing, integrated low-density switching, security, voice, IP telephony, voice mail, video, and content networking in an integrated solution. This integrated design enables enterprise customers to adapt to evolving business needs by enhancing Cisco IOS services, such as QoS, IP multicast, VPN, firewall, and an intrusion prevention system (IPS). The 3700 Series Multiservice Access Routers are based on the same modular concepts as the 3600 Series, but they enable higher levels of performance and service integration for the branch office. Go to http://www.cisco.com/go/3700 to learn more about the Cisco 3700 Series Multiservice Access Routers.

Figure 1-17 *Cisco 3700 Series*

Standalone Voice Gateways

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

Cisco VG224 and VG248 Analog Phone Gateways

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

Cisco VG200 Series Gateways include these features:

- VG200 Series Gateways are high-density gateways for using analog phones, fax machines, modems, voice-mail systems, and speakerphones.
- VG200 Series Gateways offer feature-rich functionality for enterprise voice systems based on Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.
- The VG224 Analog Phone Gateway is based on a Cisco IOS software platform and offers 24 fully featured analog ports for use as extensions to Cisco Unified Communications Manager or Cisco Unified Communications Manager Express systems in a compact 19-inch rack-mount chassis.
- The VG248 Analog Phone Gateway, as shown in Figure 1-18, offers 48 fully featured analog ports for use as extensions to the Cisco UCM system in a compact 19-inch rack-mount chassis.

Figure 1-18 *Cisco VG248*

Cisco AS5300 Series Universal Gateways

The Cisco AS5300 Series, an example of which is provided in Figure 1-19, is a series of access servers that includes the Cisco AS5350 Universal Gateway and the Cisco AS5350XM Universal Gateway. The AS5350XM Universal Gateway doubles the performance of the Cisco AS5350 Universal Gateway, allowing the same applications to run faster and with lower CPU utilization levels. Go to http://www.cisco.com/go/as5300 to learn more about the Cisco AS5300 Series Universal Gateways.

Figure 1-19 *Cisco AS5300 Series*

Cisco AS5400 Series Universal Gateways

The Cisco AS5400 Series, which is another series of access servers, includes the Cisco AS5400HPX Universal Gateway, which enhances performance for processor-intensive voice and fax applications, and the Cisco AS5400XM Universal Gateway, shown in Figure 1-20. Go to http://www.cisco.com/go/as5400 to learn more about the Cisco AS5400 Series Universal Gateways.

Cisco AS5850 Universal Gateway

The Cisco AS5850 Universal Gateway, as illustrated in Figure 1-21, is a high-density, carrier-class gateway with high capacity and availability. The AS5850 Universal Gateway is specifically designed to meet the demands of large service providers by supporting up to five channelized T3s (CT3s), 96 T1s, or 86 E1s of data, voice, and fax services on any port at any time. It offers high-availability features such as hot swap on all cards, load-sharing and redundant hot-swappable power supplies, redundant route-processing cards, and CAC to ensure 99.999 percent availability. Go to http://www.cisco.com/go/as5850 to learn more about the Cisco AS5850 Universal Gateway.

Figure 1-20 *Cisco AS5400XM Universal Gateway*

Figure 1-21 *Cisco AS5850 Universal Gateway*

Cisco 827-4V ADSL Router

The Cisco 827-4V ADSL Router, shown in Figure 1-22, provides business-class functionality for small businesses, small remote offices, and corporate teleworkers using Cisco IOS technology. It enables service providers and resellers to increase service revenue by

supporting features for business-class security, integrated toll quality voice and data, differentiated service classes, and managed network access. These features, along with the manageability and reliability of Cisco IOS, provide mission-critical networking.

Figure 1-22 *Cisco 827-4V ADSL Router*

With the software upgradeable platform of the 827-4V ADSL Router, service providers and resellers can increase revenue by offering DSL services today and provide value-added services as their customers' technology needs grow. The Cisco 827-4V ADSL Router is a member of the Cisco 800 Series Routers. Go to http://www.cisco.com/go/800 to learn more about the Cisco 800 Series Routers.

Cisco ATA 186

The Cisco Analog Telephone Adaptor 186 (ATA 186), as depicted in Figure 1-23, is a handset-to-Ethernet adaptor that allows traditional telephony devices to function as VoIP devices. Customers can use IP telephony applications by connecting their analog devices to Cisco ATAs.

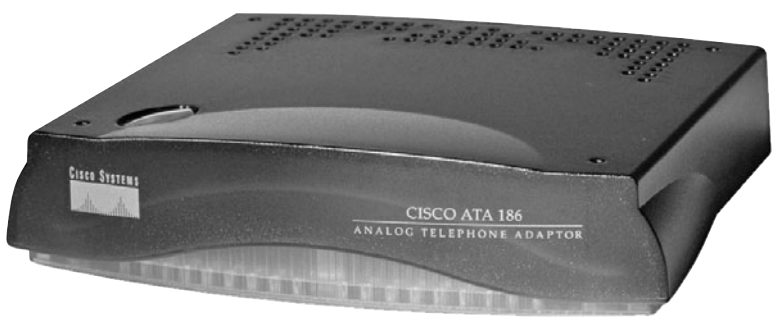


Figure 1-23 *Cisco ATA 186*

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

The Cisco Analog Telephone Adaptor 180 Series products are standards-based IP communications devices that deliver VoIP terminations to businesses and residences. Go to http://www.cisco.com/go/ata186 to learn more about the Cisco ATA 186.

Cisco 7200 Series Routers

Cisco 7200 Series Routers, an example of which is shown in Figure 1-24, are service routers for Enterprise Edge and Service Provider Edge applications. These compact routers provide serviceability and manageability coupled with high-performance modular processors such as the Cisco 7200 Network Processing Engine NPE-G1 (NPE-G1). Go to http://www.cisco.com/go/7200 to learn more about the Cisco 7200 Series Routers.

Figure 1-24 *Cisco 7200 Series Router*

Summary of Voice Gateways

Table 1-2 summarizes the Cisco voice gateway platforms.

Table 1-2 *Gateway Hardware Platforms*

Platform	H.323	Cisco Unified Communications Manager MGCP	SIP	SCCP
Cisco 827-4V	Yes	No	No	No
Cisco 2800 Series	Yes	Yes	Yes	Yes
Cisco 3800 Series	Yes	Yes	Yes	Yes
Cisco 1751-V / 1760-V	Yes	Yes	No	Yes[1]
Cisco 2600XM Series	Yes	Yes	No	No[3]
Cisco 3600 Series	Yes	Yes	No	No[3]
Cisco 3700 Series	Yes	Yes	No	No[3]
Cisco VG224	Yes[2]	Yes[2]	No	Yes
Cisco VG248	No	No	No	Yes

Table 1-2 *Gateway Hardware Platforms (continued)*

Platform	H.323	Cisco Unified Communications Manager MGCP	SIP	SCCP
Cisco AS53XX / AS5400 / AS5850	Yes	No	No	No
Communication Media Module	Yes	Yes	Yes	Yes
GW Module WS-X6608-x1 and FXS Module WS-X6624	No	Yes	No	Yes
Cisco ATA 180 Series	Yes[2]	Yes[2]	No	Yes[2]
Cisco 7200 Series	Yes	No	No	No

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

Table 1-3 offers insight into typical uses for the previously discussed voice gateways.

Table 1-3 *Gateway Model Uses*

Device/Series	Usage
Cisco 827-4V	Connect up to four analog devices via ADSL.
Cisco 2800 Series	Small- to medium-sized enterprise voice gateways.
Cisco 3800 Series	Large-sized enterprise voice gateways.
Cisco 1751-V and 1760-V	Small-sized enterprise voice gateways.
Cisco 2600XM Series	Medium-sized enterprise voice gateways.
Cisco 3600 Series	Medium-sized enterprise voice gateways.
Cisco 3700 Series	Large-sized enterprise voice gateways.
Cisco VG224	Connect up to 24 analog devices to the VoIP network.
Cisco VG248	Connect up to 48 analog devices to the VoIP network.
Cisco AS5350, AS5350XM, AS5400HPX, AS5400XM, and AS5850	Service provider voice gateway.
Communications Media Module	Provides T1/E1 and FXS interfaces and conferencing and transcoding resources on Cisco Catalyst 6500 Series Switches.
GW Module WS-X6608-x1 and FXS Module WS-X6624	Provides T1/E1 and FXS interfaces on Catalyst 6500 Series Switches.
Cisco ATA 186	Connect up to two analog devices to a VoIP network.
Cisco 7200 Series	Service provider voice gateway.

IP Telephony Deployment Models

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

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

Single-Site Deployment

The single-site model for Cisco Unified Communications consists of a call-processing agent cluster located at a single site, or campus, with no telephony services provided over an IP WAN. Figure 1-25 illustrates a typical single-site deployment. All Cisco UCM servers, applications, and DSP resources are located in the same physical location. You can implement multiple clusters inside a LAN or a metropolitan-area network (MAN) and connect them through intercluster trunks if you need to deploy more IP phones in a single-site configuration.

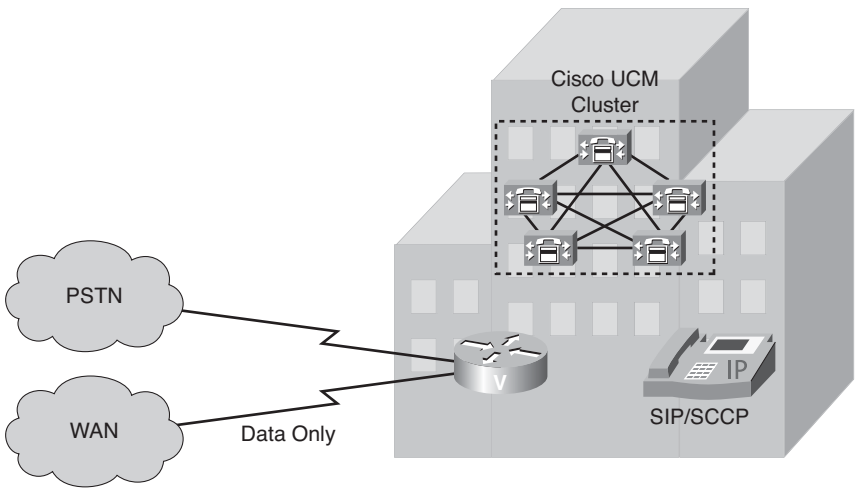


Figure 1-25 *Single-Site Deployment*

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

Design Characteristics of Single-Site Deployment

The single-site model has the following design characteristics:

- Single Cisco UCM cluster.
- Maximum of 30,000 SCCP or SIP IP phones or SCCP video endpoints per cluster.
- Maximum of 1100 H.323 devices (gateways, MCUs, trunks, and clients) or MGCP gateways per UCM cluster.
- PSTN for all calls outside the site.
- DSP resources for conferencing, transcoding, and media termination point (MTP).
- Voicemail, unified messaging, Cisco Unified Presence, audio and video components.
- Capability to integrate with legacy PBX and voice-mail systems.
- H.323 clients, MCUs, and H.323/H.320 gateways that require a gatekeeper to place calls must register with a Cisco IOS Gatekeeper (Cisco IOS Release 12.3(8)T or greater). UCM then uses an H.323 trunk to integrate with a gatekeeper and provide call routing and bandwidth management services for H.323 devices registered to it. Multiple Cisco IOS Gatekeepers might be used to provide redundancy.
- MCU resources are required for multipoint video conferencing. Depending on conferencing requirements, these resources might be either SCCP or H.323, or both.
- H.323/H.320 video gateways are needed to communicate with H.320 videoconferencing devices on a public ISDN network.
- High-bandwidth audio (for example, G.711, G.722, or Cisco Wideband Audio) between devices within the site.
- High-bandwidth video (for example, 384 kbps or greater) between devices within the site. The Cisco Unified Video Advantage Wideband Codec, operating at 7 Mbps, is also supported.

Benefits of Single-Site Deployment

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

The main benefits of the single-site model are the following:

- Ease of deployment.
- A common infrastructure for a converged solution.
- Simplified dial plan.
- No transcoding resources are required because of the use of a single high-bandwidth codec.

Design Guidelines for Single-Site Deployment

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

Best Practices for Single-Site Deployment Follow these guidelines and best practices when implementing the single-site model:

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

Multisite WAN with Centralized Call-Processing Deployment

The model for a multisite WAN deployment with centralized call processing consists of a single call-processing agent cluster that provides services for multiple remote sites and uses the IP WAN to transport Cisco Unified Communications traffic between sites. The IP WAN also carries call control signaling between central and remote sites. Figure 1-26 illustrates a typical centralized call processing deployment, with a UCM cluster as the call processing agent at the central site and an IP WAN with QoS enabled to connect all the sites. The remote sites rely on the centralized UCM cluster to handle their call processing. Applications such as voice mail and IVR systems are typically centralized as well to reduce the overall costs of administration and maintenance.

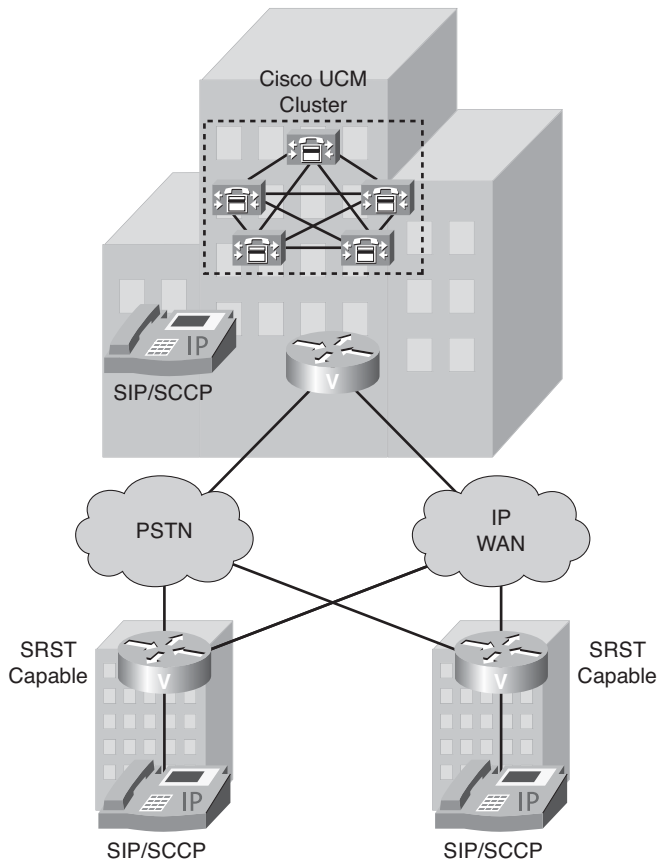


Figure 1-26 *Multisite WAN with Centralized Call Processing*

WAN connectivity options include the following:

- Leased lines
- Frame Relay
- ATM
- ATM and Frame Relay Service Inter-Working (SIW)
- Multiprotocol Label Switching (MPLS) VPN
- Voice and Video Enabled IP Security Protocol (IPsec) VPN (V3PN)

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

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

Design Characteristics of Multisite WAN with Centralized Call-Processing Deployment

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

- Single UCM cluster.
- Maximum of 30,000 SCCP or SIP IP phones or SCCP video endpoints per cluster.
- Maximum of 1000 locations per UCM cluster.
- Maximum of 1100 H.323 devices (gateways, MCUs, trunks, and clients) or 1100 MGCP gateways per UCM cluster.
- PSTN for all external calls.