cisco

Official Cert Guide

Learn, prepare, and practice for exam success

CCNA Collaboration

CIVND 210-065

BRIAN MORGAN, CCIE NO. 4865

JASON BALL

ciscopress.com

CCNA Collaboration 210-065 CIVND Official Cert Guide

BRIAN MORGAN, CCIE No. 4865
JASON BALL

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

CCNA Collaboration CIVND 210-065 Official Cert Guide

Brian Morgan, CCIE No. 4865, and Jason Ball

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

First Printing November 2015

Library of Congress Cataloging-in-Publication Number: 2015945796

ISBN-13: 978-1-58714-442-4

ISBN-10: 1-58714-442-5

Warning and Disclaimer

This book is designed to provide information about the CCNA Collaboration CIVND 210-065 exam. 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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact 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 e-mail 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

Business Operation Manager, Cisco Press: Jan Cornelssen

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Senior Development Editor: Christopher Cleveland

Project Editor: Seth Kerney

Copy Editor: Keith Cline

Technical Editors: Jhun DeLeon, Marcello Federico

Editorial Assistant: Vanessa Evans

Book Designer: Mark Shirar

Composition: Studio Galou

Indexer: Tim Wright

Proofreader: Megan Wade-Taxter

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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 Authors

Brian Morgan, CCIE No. 4865, is a consulting systems engineer with Cisco specializing in collaboration technologies. In over 20 years in the networking industry, he has performed in a number of roles, including pre- and post-sales engineering, network consultant, Certified Cisco Systems Instructor, and engineering director for a telecommunications company. When he is not spending time with family and friends, Brian enjoys working with local high school and college students participating in local Cisco Network Academy programs, as well as STEM and FIRST Robotics programs in North Texas.

Jason Ball is married to his beautiful bride of 18 years, Siobhan Ball. They have two children, Isaac and Maureen. Both children have caught his passion for the technology industry. They are both involved in a robotics program through FIRST Lego League, with his wife coaching both their teams. Through this program, they learn skills like programming, electrical engineering, mechanical engineering, civil engineering, and other skills like gracious professionalism. Outside of this program, his daughter is getting into software design, and his son is taking courses through North Carolina State University called Young Engineers, offered for children between 12 and 18 years of age, where he is furthering his IT skills.

Jason was a slow starter in the IT industry. His beginnings date back to 1989 with an opportunity to work with audio/video systems. In 1993, his focus changed to public speaking. He traveled around for many different types of speaking engagements, encountering groups of varying ages. In 2003, he was introduced to multicast media. This unfamiliar and exciting opportunity rekindled a desire for involvement in technology.

In 2009, a new opportunity presented itself. Jason was recently unemployed when a connection with Scott Waschler, an employee at TANDBERG, opened a door to contract as a technical trainer. In May 2010, Cisco purchased TANDBERG, and a new world of technology emerged. This is a journey that will never end, and Jason is continually hungry to learn all he can and to share that knowledge with others who are also eager to learn.

Jason currently works for Compass Business Solutions, a Learning Partner of Cisco. Compass specializes in teaching Collaboration-related courses, including CIVND 2. He holds many certifications, most of which are with Cisco. His current certifications with Cisco include CCNA Route/Switch, CCDA, CCSI, CCNA Video, CCNA Voice, CCNA Collaboration, CCNP Voice, CCNP Collaboration, CSE, LVCI, BACI, Cisco Video Network Specialist, and TVS Certified Specialist.

About the Technical Reviewers

Jhun DeLeon is an industry veteran when it comes to voice, video, and data networking, having deployed numerous complex TelePresence/videoconferencing projects for large companies with global presence. When Cisco started selling TelePresence solutions, Jhun shifted his focus to TelePresence, or what is called collaboration. Jhun worked at Cisco System as a voice engineer working on unified communications. After Cisco, Jhun has worked with Cisco Partners doing design, architecture, and implementation of unified communications, TelePresence, videoconferencing, digital signage, and physical video surveillance.

Marcello Federico is a technical leader in the Cisco Collaboration Technology group, focused on video technologies and collaboration APIs. He is currently a consulting systems engineer covering the Pacific Northwest Enterprise segment where he works with his customers on creating their unified communications architecture and strategy. Prior to Cisco, Marcello held various systems engineering roles focused on the Enterprise, selling DSP media processing blades, software SDKs, and API stacks. Marcello graduated from the University of Western Ontario and obtained a degree in computer science with a specialization in software engineering. He loves to write code and continues to learn about the latest programming techniques and how to apply them to the Cisco collaboration APIs. He lives in Seattle, WA with his wife, Denise; children, Domenic and Cole; and his trusty old cattle dog, Chester. In his spare time he enjoys playing soccer and golf and spending time with his family.

Dedications

Brian Morgan: This book is dedicated to Sunshine and the pursuit of much and more.

Jason Ball: To my wife, Siobhan. I couldn't do what I do if you didn't do what you do.

Acknowledgments

Brian Morgan: This book would not have been possible without the support and assistance of my awesome team in SLED West Collaboration, in particular Mike Popovich and Luc Bouchard. Their willingness to accommodate the erratic schedule (and moodiness) that has accompanied the writing of this book has left me astounded.

A huge thank-you is not nearly sufficient for the efforts, patience, guidance, and professionalism of the editorial team: Brett Bartow and Christopher Cleveland.

Most of all, I want to thank my co-author, Jason Ball. He is, without a doubt, the master of the diving catch.

Jason Ball: Special thanks must be given to James Lehto, who helped open the door for me to write this book. My co-author, Brian Morgan, has proven to be a great asset and a new friend. Thanks must also go out to Brett Bartow and Christopher Cleveland for their patience and proficiency throughout this process.

My co-worker, Jeff Hubbard, has been an invaluable asset, sounding board, and punching bag for me to abuse while writing this book. If he had to hear me say "I'm writing this book" one more time, I might have become the punching bag. You have proven to be a great friend, and for that I am truly grateful.

Finally, I must acknowledge my wife. You have been more supportive than I could have ever asked. You have carried the slack, encouraged me, and pressed me at exactly the times that I needed it. The success of this book is as much to your credit as it is to mine.

Contents at a Glance

Contents

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.

Introduction

Professional certifications have been an important part of the computing industry for many years and will continue to become more important. Many reasons exist for these certifications, but the most popularly cited reason is that of credibility. All other considerations held equal, the certified employee/consultant/job candidate is considered more valuable than one who is not.

Goals and Methods

The most important, and somewhat obvious, goal of this book is to help you pass the CCNA Collaboration CIVND exam (210-065). In fact, if the primary objective of this book were different, the book's title would be misleading; however, the methods used in this book to help you pass the CCNA Collaboration CIVND exam are designed to also make you much more knowledgeable about how to do your job. Although this book and the accompanying CD together have more than enough questions to help you prepare for the actual exam, the method in which they are used is not to simply make you memorize as many questions and answers as you possibly can.

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. So, this book does not try to help you pass by memorization, but helps you truly learn and understand the topics. The CCNA Collaboration CIVND exam is just one of the foundation topics in the CCNA Collaboration certification, and the knowledge contained within is vitally important to consider yourself a truly skilled routing/switching engineer or specialist. This book would do you a disservice if it did not attempt to help you learn the material. To that end, the book will help you pass the CIVND exam 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
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the CD

Who Should Read This Book?

This book is not designed to be a general networking topics book, although it can be used for that purpose. This book is intended to tremendously increase your chances of passing the CCNA Collaboration CIVND exam. Although other objectives can be achieved from using this book, the book is written with one goal in mind: to help you pass the exam.

So why should you want to pass the CCNA Collaboration CIVND exam? Because it is one of the milestones toward getting the CCNA Collaboration certification (no small feat in itself). What would getting the CCNA Collaboration mean to you? A raise, a promotion, recognition? Would it enhance your resume? Perhaps it would demonstrate that you are serious about continuing the learning process and that you are not content to rest on your laurels. Maybe it would please your reseller-employer, who needs more certified employees for a higher discount from Cisco. Or one of many other reasons.

Strategies for Exam Preparation

The strategy you use for the CCNA Collaboration CIVND exam might be slightly different from strategies used by other readers, mainly based on the skills, knowledge, and experience you already have obtained. For instance, if you have attended the CICD and CIVND courses, you might take a different approach than someone who learned collaboration architecture via on-the-job training.

Regardless of the strategy you use or the background you have, the book is designed to help you get to the point where you can pass the exam with the least amount of time required. For instance, there is no need for you to practice or read about IP addressing and subnetting if you fully understand it already. However, many people like to make sure that they truly know a topic and therefore read over material that they already know. Several book features will help you gain the confidence that you need to be convinced that you know some material already, and to also help you know what topics you need to study more.

210-065 CIVND Exam Topics

Table I-1 lists the exam topics for the 210-065 CIVND exam. This table also lists the book parts in which each exam topic is covered.

Table I-1 210-065 CIVND Exam Topics

CICD 210-065 Exam Topic	Chapters in Which Topic Is Covered
1.0 Video Concepts	
1.1 Describe the functional components of video solutions	
1.1.a Provisioning and scheduling management	Chapters 9, 17
1.1.b Video compositing	Chapter 2
1.1.c Streaming video	Chapter 2
1.1.d Recording and storage	Chapter 2
1.1.e Media players	Chapter 2
1.1.f Media convergence	Chapter 2
1.1.g Media management	Chapter 2
1.1.h Video convergence	Chapter 4
2.0 Endpoint Configuration	
2.1 Describe video product models	
2.1.a Mobile devices	Chapter 5
2.1.b Desktop systems	Chapter 5
2.1.c Multi-purpose systems	Chapter 5
2.1.d Surveillance cameras and encoders	Chapter 3
2.1.e Immersive systems	Chapter 7
2.1.f Peripherals and add-ons	Chapter 7
2.1.g Cabling connections	Chapter 7
2.1.h Digital media players	Chapter 2
2.2 Describe environment recommendations	
2.2.a Room lighting recommendations	Chapter 8
2.2.b Room acoustics recommendations	Chapter 8
2.2.c Room power recommendations	Chapter 8
2.2.d Room HVAC recommendations	Chapter 8
2.2.e Room materials (windows, floor material, wall material, etc.)	Chapter 8
2.2.f Room size and background wall	Chapter 8
2.2.g Viewing distance	Chapter 8

CICD 210-065 Exam Topic	Chapters in Which Topic Is Covered
2.2.h Physical security recommendations	Chapter 3
2.3 Implement desktop endpoints and surveillance cameras	
2.3.a Network settings	Chapter 5
2.3.b GUI interface and CLI	Chapter 5
2.3.c Control plane	Chapter 5
2.3.d Cables	Chapter 5
2.3.e Test call	Chapter 6
2.3.f User acceptance test	Chapter 6
2.3.g Microphone calibration	Chapter 6
2.3.h Camera calibration	Chapter 6
2.3.i Media playback on PCs	Chapter 6
2.4 Describe features and functions	
2.4.a Auto collaboration	Chapter 11
2.4.b MCU capabilities versus TelePresence Server	Chapters 14, 15, 16
2.4.c Audio add in	Chapter 11
2.4.d PIP	Chapter 11
2.4.e FECC	Chapter 11
2.4.f Resolution setting	Chapter 11
2.4.g Multiway versus multisite	Chapter 14
3.0 Troubleshooting and Support	
3.1 Describe troubleshooting methodologies	Chapter 13
3.2 Identify endpoint issues	
3.2.a Cabling	Chapter 13
3.2.b Peripherals	Chapter 13
3.2.c Network connectivity	Chapter 13
3.2.d Registration	Chapters 6, 8, 9, 10
3.2.e Call setup	Chapters 6, 10, 11, 12

CICD 210-065 Exam Topic	Chapters in Which Topic Is Covered
3.2.f Media quality	Chapter 13
3.2.g Mid call feature issues	Chapters 10, 13
3.3 Collecting system information	
3.3.a Logs	Chapter 13
3.3.b Status	Chapters 6, 13
3.4 Manage configuration	
3.4.a Backups	Chapters 10, 13
3.4.b Restore	Chapters 10, 13
3.4.c Reset to defaults	Chapters 10, 13
3.4.d Password recovery	Chapters 10, 13
3.5 Implement key CLI commands	Chapter 13
3.6 Monitor events and alerts	Chapter 13
4.0 Conferencing Concepts	
4.1 Describe multipoint control units	Chapter 15
4.2 Describe conferencing features	
4.2.a Switching and layout options	Chapters 10, 14, 15, 16
4.2.b Cascading	Chapters 14, 15, 16
4.2.c Conferencing add-ons	Chapters 14
4.3 Describe scheduling versus adhoc versus on demand features	Chapters 17

CCNA Collaboration CIVND 210-065 Official Certification Guide

The objective of this book is to help you pass the CCNA Collaboration CIVND exam (210-065). While you are learning about topics that can help you pass the CIVND exam, you will also become more knowledgeable about how to do your job. Although this book and the accompanying CD have many exam preparation tasks and example test questions, the method in which they are used is not to simply make you memorize as many questions and answers as you possibly can.

The methodology of this book helps you discover the exam topics about which you need more review, fully understand and remember exam topic details, and prove to yourself that you have retained your knowledge of those topics. So this book helps you pass not by memorization, but by helping you truly learn and understand the topics. The

CIVND exam is just one of the foundation topics in the CCNA Collaboration certification, and the knowledge contained within is vitally important to consider yourself a truly skilled Cisco Collaboration engineer or specialist.

The strategy you use to prepare for the CIVND exam might be slightly different from strategies used by other readers, mainly based on the skills, knowledge, and experience you already have obtained. For instance, if you have attended the CIVND course, you might take a different approach than someone who learned switching through on-the-job training. Regardless of the strategy you use or the background you have, this book is designed to help you get to the point where you can pass the exam with the least amount of time required.

Book Features and Exam Preparation Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, 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.

The book includes many features that provide different ways to study so that you are ready for the exam. If you understand a topic when you read it but do not study it any further, you will probably not be ready to pass the exam with confidence. The features included in this book give you tools that help you determine what you know, review what you know, better learn what you do not know, and be well prepared for the exam. These tools include the following:

- **"Do I Know This Already?" quizzes:** Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying that chapter.
- **Foundation topics:** These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- **Exam preparation tasks:** The "Exam Preparation Tasks" section lists a series of study activities that should be done after reading the "Foundation Topics" section. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include the following:

  - **Key topics review:** The Key Topic icon is shown next to the most important items in the "Foundation Topics" section of the chapter. The Key Topics Review activity lists the key topics from the chapter and page number. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic. Review these topics carefully.
  - **Memory tables:** To help you exercise your memory and memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the CD. This document lists only partial information, allowing you to complete the table or list. CD-only Appendix C holds the incomplete tables, and Appendix D includes the completed tables from which you can check your work.

- **Definition of key terms:** Although Cisco exams might be unlikely to ask a question such as "Define this term," the CIVND exam requires that you learn and know a lot of networking terminology. This section lists some of the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary at the end of the book.

- **CD-based practice exam:** The companion CD contains an exam engine, including a bank of multiple-choice questions. You can use the practice exams to get a feel for the actual exam content and to gauge your knowledge of switching topics.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. Chapters 1 through 17 are the core chapters and can be covered in any order. If you do intend to read them all, the order in the book is an excellent sequence to use.

The core chapters, Chapters 1 through 17, cover the following topics:

- **Chapter 1, "Introduction to Video Communications"**—This chapter discusses Cisco collaboration architecture from the perspective of prescriptive design using the Cisco Preferred Architecture documentation available at Cisco.com.

- **Chapter 2, "Cisco Digital Media and Content Delivery"**—This chapter wanders back in time for a brief history lesson on legacy digital media architecture. It then moves back into the twenty-first century to discuss the Cisco Digital Media Suite, Digital Signs, Cisco Cast, and Show and Share.

- **Chapter 3, "Cisco Video Surveillance"**—This chapter takes a look at video from a physical security standpoint. The discussion covers legacy closed-circuit television, Cisco's physical security solutions, and Cisco video-surveillance components and architectures.

- **Chapter 4, "Cisco Collaboration Overview"**—This chapter examines the evolution of videoconferencing, beginning with legacy videoconferencing architectures and working forward to today's Cisco collaboration solutions. This discussion includes an overview of the Cisco collaboration components and general collaboration architecture.

- **Chapter 5, "Cisco IP Phones, Desktop Endpoints, and Jabber Overview"**—As the title implies, this chapter focuses on the Cisco collaboration endpoint portfolio. This includes current Cisco IP Phones, desktop units, and Cisco Jabber.

- **Chapter 6, "Configuring Cisco Unified IP Phones and Cisco Jabber"**—This chapter focuses on the configuration of Cisco IP Phones both in Cisco Unified Communications Manager and on the phones themselves. It describes the requirements for phone registration and how to verify phone status information. Also

included in this chapter is a breakdown of the configuration and registration of Cisco Jabber. This includes the client installation, configuration (on both the client side and CUCM side), and verification.

- **Chapter 7, "Cisco TelePresence Endpoint Characteristics and Installation"**—This chapter discusses the Cisco TelePresence endpoint portfolio, including desktop units such as the EX and DX series endpoints and room-based and immersive endpoints. In addition, this chapter covers intelligent proximity features available on newer endpoints. There is some discussion of Cisco TC software components and deployment, C series codec configuration options, and the Cisco Jabber Video for TelePresence client (formerly known as Movi).
- **Chapter 8, "Configuring Cisco TelePresence CTS Software-Based Endpoints"**—This chapter focuses on the setup and configuration of Cisco TelePresence Server-based endpoints and on user provisioning for their use.
- **Chapter 9, "Configuring Cisco DX650 Endpoints"**—This chapter goes into the setup and configuration of Cisco's new collaboration desktop experience endpoint, the DX650. This is a dramatic departure from Cisco's traditional endpoint look and feel, creating an entirely new user experience. This chapter discusses the operating system, parameter configurations, and how to register the endpoint with CUCM.
- **Chapter 10, "Configuring Cisco TelePresence TC Software-Based Endpoints"**—This chapter discusses the installation, configuration, and troubleshooting of Cisco TelePresence TC software-based endpoints. This includes code upgrades, peripheral calibration, and how to enable intelligent proximity. These endpoints are capable of utilizing the Cisco Touch series control panels. So, there is some discussion of Touch panel configuration. In addition, this chapter walks through available call control options and configuration using both SIP and H.323 protocol options. These options include near- and far-end camera control, media encryption, mobility, and the configuration and deployment of Cisco Jabber Video for TelePresence (Movi).
- **Chapter 11, "Cisco Legacy Edge Architecture"**—This chapter provides something of an evolutionary picture of Cisco's edge access architecture. This includes the concepts of firewall traversal and video call control, both inside the network and outside. This chapter then discusses Cisco's newest edge architecture, known as Expressway, sometimes called collaboration edge. It is an evolution of firewall-traversal technologies to include a wide range of collaboration services in order to provide a seamless, VPN-less user experience. This chapter covers the components of the architecture, the mobile and remote access solution, and Cisco Jabber Guest.
- **Chapter 12, "Operating and Troubleshooting Cisco TelePresence Endpoints"**—This chapter focuses on what to do when things may not be working as planned or expected. The discussion covers the collection of logs and status information from TC software-based endpoints, TC software configuration and maintenance, and issue identification/isolation. The discussion then shifts focus to Cisco TelePresence CTS endpoints for the same discussion points. Closing out the chapter is a discussion on troubleshooting and problem reporting on the DX650 and issue identification/isolation for Cisco the Jabber Video for TelePresence (Movi) client.

- **Chapter 13, "Cisco Multipoint Solution"**—This chapter digs into the products and solution components involved in deploying multipoint, multisite, and multiway videoconferencing features.
- **Chapter 14, "Cisco TelePresence MCUs"**—This chapter describes the purpose, configuration, deployment, and use of Cisco TelePresence MCU hardware.
- **Chapter 15, "Cisco TelePresence Server"**—This chapter discusses the installation, configuration, and deployment of Cisco TelePresence Server in both VCS and CUCM call control environments.
- **Chapter 16, "Cisco TelePresence Management Suite"**—This chapter provides a look into TMS for endpoint provisioning and management, conference resource scheduling and management, and videoconference monitoring and reporting.
- **Chapter 17, "Cisco WebEx Solutions"**—This chapter discusses Cisco WebEx Meeting Center for cloud-based web, audio, and videoconferencing. Cisco WebEx Meeting Center also includes the ability to allow for screen sharing, remote control, file transfer, whiteboarding/annotation, and recording of conferences.

In addition to the 17 main chapters, this book includes tools to help you verify that you are prepared to take the exam. Chapter 18, "Final Preparation," includes guidelines that you can follow in the final days before the exam. Also, the CD-ROM includes quiz questions and memory tables that you can work through to verify your knowledge of the subject matter.

In addition, you can find the following appendixes on the CD that is included with this book:

- Appendix C, "Memory Tables," holds the key tables and lists from each chapter with some of the content removed. You can print this appendix, and as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exams.
- Appendix D, "Memory Table Answer Key," contains the answer key for the exercises in Appendix D.
- Appendix E, "Study Planner," is a spreadsheet with major study milestones, where you can track your progress through your study.

For More Information

If you have any comments about the book, you can submit those at Cisco.com. Just go to the website, select **Contact Us**, and type in your message.

Cisco might make changes that affect the CIVND exam from time to time. You should always check http://www.cisco.com/web/learning/certifications/associate/index.html for the latest details. Register your product at ciscopress.com/register for convenient access to downloads, updates, and corrections as they become available.

This page intentionally left blank

This chapter covers the following topics:

- **Video Use Cases:** This section provides a brief discussion of potential use cases for video.
- **Architectural Overview:** This section provides a high-level view of the core components of Cisco video solutions.

CHAPTER 1

Introduction to Video Communications

High-quality, immersive video capabilities provide what may be the single most transformative technology available today. Through the use of prescriptive best practices, Cisco has pushed video into the technological spotlight. These prescriptive recommendations are made available on Cisco.com as *Cisco Preferred Architecture* guides. These preferred architecture guides are written specifically for design and deployment engineers and are referenced throughout this book.

Video has long been seen as a gimmick technology, at best. A number of conditions have contributed to the view that video is simply not viable as a communication medium. Thankfully, the current generation of video technologies and offerings has greatly changed that view. This chapter provides an overview of potential video use cases and architecture.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 1-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 1-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Video Use Cases	1–2
Architectural Overview	3–5

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What is a SIP URI?
   a. An email address
   b. A globally unique identifier utilized for SIP dialing
   c. A user's Microsoft Active Directory credentials
   d. The address typed into a browser to reach a web page
2. What is the minimum requirement to establish a conference call (audio or video)?
   a. A URI
   b. A URL
   c. Bridging resources
   d. Internet connectivity
3. Which Cisco video architecture component provides the foundation for all other components?
   a. Call control
   b. Endpoints
   c. Conferencing
   d. Collaboration edge
   e. Applications
4. Which Cisco video architecture component is responsible for the success or failure of the user experience?
   a. Call control
   b. Endpoints
   c. Conferencing
   d. Collaboration edge
   e. Applications
5. Which Cisco video architecture component allows for VPN-less access and is responsible for interoperability functions?
   a. Call control
   b. Endpoints
   c. Conferencing
   d. Collaboration edge
   e. Applications

Foundation Topics

Video Use Cases

Businesses are struggling to find ways to remain relevant with their employees, peers, competitors, stockholders/investors, and customers. This can necessitate a somewhat delicate balancing act when faced with cost cutting, productivity improvement, and innovation requirements. First and foremost, it should be stated that achieving this balance is possible.

In one form or another, video technologies are garnering excessive amounts of attention. It is worth noting that consumer video software is not the focus of this discussion or this book. Consumer-grade video software simply does not have the capability to offer the immersive, in-person-experience quality necessary in business. Typically, such software clients are highly unsecure, as well, and may be banned/blocked by business and firewall policies.

The use cases for video are many and diverse. What follows is merely a cross-section of the possibilities for transforming the way business is done within your organization. Among the examples to be discussed are the following:

- Video as an extension of telephony
- Video meetings and conferences
- Extending video communications to teleworkers
- Video contact center

The purpose of discussing these cases is simply to get your mind moving in the direction of thinking of video as something more than a tool or a novelty. In doing so, you become more open and adept at understanding and explaining the pervasive transformative possibilities it offers.

Video as an Extension of Telephony

The overarching view Cisco has taken toward video is that it should be as intuitive as using a legacy telephone. An often-heard phrase in recent years is, "Video is the new dial tone." That simple statement sums up the ease-of-use drive that has given video technologies some much-needed advances in recent years. All that is needed is a video-capable endpoint. No additional knowledge or training is required to make use of video functionality. One simply needs to make a phone call. If both ends are video capable, it will work.

Thankfully, gone are the days when only the IT guys could set up and initiate a video meeting. Now, it is as easy as touching a button or clicking a mouse. Using video is no more difficult or labor intensive than using your desk phone or smartphone to place an audio call. In fact, there is really no longer any real need to remember phone numbers in the traditional sense. Video calling can certainly be accomplished by dialing digits, of course. But, it is more easily accomplished through the use of a Uniform Resource Identifier (URI). A URI is a Session Initiation Protocol (SIP) address to which a call can be routed. The URI takes the format user@domain.com. Together, these create a globally unique identifier for the user in question. The URI is not an email address, but it is usually matched to the email alias of the individual at the video endpoint you want to dial for purposes of simplicity.

With video integrated into the desk phone, either directly or through the use of Cisco Jabber (with desk phone control and a webcam), the user experience is greatly enhanced. Face-to-face communication tends to be more productive and consistently engaging than audio only. One side effect of video, for better or worse, is a reduction in multitasking. Conversations and interactions are more productive simply by virtue of making eye contact with a colleague in the next office or half a world away. All communications within the office can now be face to face. Of course, the option always exists to mute the video on a bad hair day.

Video Meetings and Conferences

There was a time when the very mention of a videoconference spread fear, uncertainty, and doubt among attendees and IT personnel alike. Videoconferencing can be accomplished in a number of ways. As an extension of telephony, a conference call is a conference call. In traditional telephony, there is usually talk of basic conferencing in the form of ad hoc or meet-me capabilities. The minimum requirements for an audio conference is, simply put, some kind of bridging resource. The same holds true for videoconferences. The process to initiate them is identical. In an ad hoc (or instant) conference, a point-to-point call is established, followed by one party initiating the addition of the other attendees. For a meet-me conference, all parties dial a predetermined number and join an already existing bridge. Again, there is no difference when using video-capable endpoints.

Where videoconferencing used to create cringeworthy responses was in the meeting room. The dreaded rolling television with a pseudo-cam on top of it and an ISDN connection that could only be initiated by individuals with specialized knowledge has become a symbol of everything the video user experience should not be. User adoption was further hampered by the inability for end users to schedule, manage, or initiate their own conference calls. The IT department was always required to accomplish any video-related resources. There was no real concept of true collaboration. Documents had to be manually distributed to meeting attendees before meeting time. Videoconferencing has become fluid and effortless using one-touch, or in some cases zero-touch, initiation/join. These so-called immersive systems provide an in-person experience second to none. In fact, in many ways, providing just the right immersive video experience may be better than being there. Features such as Proximity, which allows meeting attendees to follow shared content from mobile devices (including screenshot and scroll-back capabilities for presentations), add a facet to meetings not previously considered a viable possibility short of asking for the presentation to be emailed out and possibly asking the presenter to back up a slide or two. With Proximity, attendees can simply grab the pieces they want or scroll through the slides on a mobile device.

Extending Video Communications to Teleworkers

As businesses search for new ways to remain profitable and reduce expenses, more and more are turning away from traditional brick-and-mortar office space for some or all of their workforce. With Cisco collaboration technologies, you can place video communications capabilities in the home or remote offices of teleworker employees. This provides the in-office experience while eliminating the need for those workers to use corporate-owned office space. The morning and evening commute now consists solely of the walk from one part of the home to the other, in many cases.

Teleworker architectures are by no means a one-size-fits-all proposition. The solution architecture varies along with the job function of said teleworker. Advanced teleworkers may require fully functional contact center agent capabilities, immersive video endpoints, and more. Hybrid teleworkers may spend only a percentage of time in the office and the rest of their time in the remote/home office. Other teleworkers may be fully mobile and always on the go.

Each of these possibilities carries with it a specific set of highly secure and reliable architectures, which include some mix of virtual private networking (VPN), web access, voice/video capabilities, and other potential technologies required to fulfill the job function in question. Video contact center agents, immersive TelePresence, desktop video, desk phone video, soft phone video, streaming video, and so on are all possible requirements that can be easily implemented for any type of teleworker.

Video Contact Center

The use of contact center agents is an extremely well-established means of servicing and maintaining contact with customers. In today's world, we often encounter an increasingly negative view of contact centers. Poorly designed scripts, inefficient interactive voice response (IVR) designs, and a score of other issues have caused a revolt of sorts by customers. People calling into customer service lines now want to quickly speak to a representative, instead of trying to navigate the menus in an attempt to find what they seek.

As more and more customers, clients, and peer businesses acquire video capability, it is easy to see where the video contact center agent may come into play. Using a solutionsuch as Cisco Remote Expert, customers and agents can engage in a more interpersonal discussion. This allows a level of collaboration far superior to the traditional contact center.

When customers call a business, they not only get to speak to a representative, they also get to make eye contact and interact face to face, just as if they were in the same room. This proves especially valuable in high-touch or white-glove customer service-focused institutions, such as high-end banking. When large amounts of money are being deposited and withdrawn, it behooves a financial institution to provide that extra touch of technology and professionalism to make a customer feel more at ease with the decision to do business with them. Seeing and speaking to a person provides the in-person experience customers are demanding from businesses today.

Business-to-Business Video

As video adoption increases and accelerates, it becomes pervasive within an enterprise. In other words, it becomes the norm. It simply becomes that which is expected in all business-related interactions. Internally, this doesn't typically pose much of an issue because all that is required is a video-capable endpoint and a means of reaching it across the network. Obviously, there is a bit more to it than that, architecturally. More on that as the book progresses.

When business is done face to face, collaboration becomes natural. Escalation of instant messages to video calls or videoconferences can be done in a click. These same tools start to become an expectation in all dealings with peers, colleagues, partner companies, customer companies, and on down to the individual customer. Business-to-business (B2B) video is a

relatively uncomplicated extension of the existing video architecture. That is, assuming both sides are using standards-compliant (not merely standards-based) endpoints/architectures. Proprietary endpoints, codecs, architectures, and so on will not be able to easily participate in such communications unless both sides have deployed said proprietary solution.

The value of B2B video comes from being able to easily and seamlessly collaborate with business contacts in real time using more personal, effective means than simply audio calling and email. Adding video, instant messaging, content sharing, file transfer, and other features increases productivity immensely.

Architectural Overview

Like any true architecture, Cisco video architectures consist of layers of components. The architecture includes a number of components working in concert to provide the desired user features and experience. In addition, the architecture provides high availability and security. By implementing these components and services, it becomes rather simple to implement any of the video use cases mentioned earlier because they are all extensions of a common system. Figure 1-1 shows an overview of the architectural components.

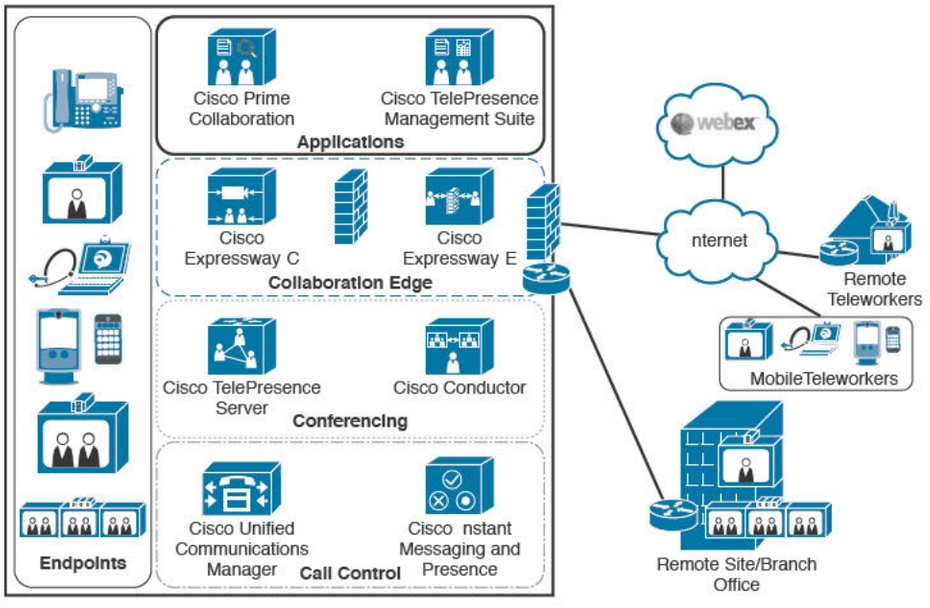


Figure 1-1 *Cisco Video Architecture Overview*

The figure shows the relationship and modularity of the various components discussed in this chapter. Each set of components is layered on top of the other components, and the endpoints make use of the features and functions provided at all levels. Also noted in the figure are the remote sites and teleworkers mentioned earlier in this chapter. Once the architectural components are in place, adding more endpoints, regardless of location, requires only the endpoints to be added at each site. Table 1-2 provides some detail on the components and the purpose of each.

Table 1-2 Components in the Cisco Video Architecture

Module	Component	Function
Call control	Cisco Unified Communications Manager (CUCM)	Endpoint registration, call processing, media resources
	CUCM IM and Presence	Instant messaging and presence
	Cisco Integrated Services Router (ISR)	Survivable Remote Site Telephony (SRST)
Endpoints	Cisco Jabber, desktop video, and TelePresence units	Real-time voice, video, content, and desktop share for users
Conferencing	Cisco TelePresence Conductor	Manages conferencing ports, parameters, and resources
	Cisco TelePresence Server	Audio and videoconferencing resources (virtual server)
Collaboration edge	Expressway-C	Interoperability and firewall traversal
	Expressway-E	Remote endpoint registration to CUCM and B2B communication
	Cisco TelePresence ISDN Gateway	Interoperability with H.320 endpoints
Applications	Cisco Prime Collaboration	Provisioning, monitoring, management, analytics
	Cisco TelePresence Management Suite (TMS)	Scheduling, web conference integration, advanced video features
	Cisco TMS Suite Extension for Microsoft Exchange	Enables TMS scheduling via Microsoft Outlook

Call Control

Call control is the component that provides the foundation of the video architecture. In essence, it is the single most important function. Without call control, there is no solution. Call control is more than just a signaling mechanism. It handles endpoint registration, dial plan, called and calling party presentation, call admission control, codec selection, and trunking operations. There is quite a bit more that goes on with CUCM, in particular.

From a video architecture perspective, CUCM provides the common platform for voice and video endpoint registration and management. This includes soft phone, desk phone, desktop video endpoints, and immersive TelePresence endpoints. Cisco has made great strides in consolidating all elements into a single call control entity to ease overall administration tasks.

In addition, the instant messaging and presence (IM&P) capabilities have been rolled into CUCM from an administrative standpoint. Although the Cisco Unified Presence Server (CUPS) is still a separate virtual server, once installed, it is administered through the CUCM

administrative web page. This allows a single pane of glass for call control and for IM, network-based presence, federation, and the use of Cisco Jabber on desktop and mobile devices.

Endpoints

There has been a slight shift in nomenclature as it pertains to collaboration architecture. Where the collaboration architecture used to reference phones and calls, it now references endpoints and sessions. An endpoint is no longer necessarily merely a phone. The endpoint may be any phone or video device in the Cisco portfolio, be it a 3905, 8861, DX80, or MX700. From an administrative perspective, they are all identical in how they are configured in CUCM. That said, a call is no longer necessarily audio only. The term *session* provides a more generic descriptor while carrying the same essential connotation.

With the diversity of the endpoints available comes a diversity in features that each may access and use. With call control and endpoints in play, the remaining pieces of the architecture provide modularity in functionality. Whereas call control provides a foundation, endpoints provide a means of accessing the wide array of services and applications available within the remaining architectural components. The endpoint is the face of the system as it provides the user experience. If the endpoint is difficult to use or complicated to deploy, there may be a high potential for adoption and growth problems.

Conferencing

A conference is loosely defined as three or more people communicating in real time. This is a core capability of legacy voice deployments and video deployments. The ability to communicate only via point-to-point video will have a negative impact on adoption of the technology. If video is the new way, it needs to function in a similar manner to the old way, with very little, if any, learning curve.

Conferencing capabilities build upon the existing infrastructure for point-to-point calls. For multiparty calls, additional resources will be required. The idea, however, is to offer the same ease of use and consistent experience regardless of how many individuals are in attendance. This is accomplished by positioning the right components within the network. These components are sized based on usage expectations and user habits. Participants can join from any standards-compliant video endpoint using standard definition (SD), high definition (HD), High Definition Plus (HD+), or a higher-end resolution known as FullHD (more on those later in the book). As adoption grows, it may well become necessary to expand the resources available for conferencing.

Conferences can be classified into three types:

- **Ad hoc (instant):** This is a conference that is not scheduled. It begins as a point-to-point call. Once established, one party or the other adds additional participants.
- **Personal (persistent):** Formerly known as a rendezvous bridge, personal meeting rooms are static meeting spaces defined on a per-user basis. These rooms can be allocated to executives, power users, or anyone else who requires it. Cisco Collaboration Meeting Rooms (CMR) are persistent meeting rooms that can be joined by dialing a URI and clicking a hyperlink in an invitation email (which launches WebEx) or by simply dialing

the pilot phone number and entering the meeting number. Like other WebEx meetings, CMR meetings can be joined from the WebEx client on any mobile device. Other terms that might describe a personal meeting room include *meet-me* and *static bridges*.

- **Scheduled (meet-me):** A conference call planned in advance. The start time and resources needed are set ahead of time. For scheduled conferences, generally, the required conferencing resources are reserved and guaranteed available at start time.

As noted in Figure 1-1, conferencing uses the Conductor and TelePresence server. The TelePresence server handles the audio/video portion of the conference. The Conductor coordinates resources for conferences. It has the ability to cascade across bridges and allocate resources best suited for the types and needs of attending clients (SD/HD/HD+/FullHD, and so on) even if those resources are not collocated.

Collaboration Edge

Businesses have long struggled to find the most efficient way to provide secure, reliable services to their user communities working outside of the traditional office setting. The bring-your-own-device (BYOD) movement has done little more than increase the pressure to find innovative access methodologies which provide the necessary access to services and applications while aligning to business and security policies.

Collaboration edge is a new implementation of an existing technology, firewall traversal. This mechanism allows Cisco to provide mobile/remote access to teleworkers without the need for a VPN connection or additional licensing typically associated with that connection. The solution consists of two core components: Expressway-E and Expressway-C. Expressway-E acts as a traversal server for external clients, video endpoints, and so on. It will be the device also in charge of handling B2B calls and cloud connectivity (WebEx). Expressway-C acts as the traversal client. It creates outbound connections to the Expressway-E (and therefore through the firewall without need to open specific ports). The firewall traversal mechanism opens a connection through the Expressway-E, across the firewall to the Expressway-C, and then on to the other relevant components as requested by the mobile client.

In Figure 1-1, the architecture shows the Expressway-C on the internal network; the Expressway-E sits in the demilitarized zone (DMZ) to handle external requests coming in. The connectivity is established from the remote clients to the Expressway-E using Domain Name System (DNS) Service (SRV) records. When the user launches a client from a mobile device or laptop, the DNS lookup resolves the records for services required by the client application and makes contact. Registration is processed, and the user is able to log in successfully.

It is suggested that the Expressway-E and Expressway-C be deployed in a highly available configuration (that is, in clustered pairs). This ensures that services are always available even when there may be network-related issues in progress. Optionally, an ISDN gateway can be deployed in support of legacy H.320 endpoints. The collaboration edge architecture also enables native interoperability with Microsoft Lync audio and video. This allows Expressway-C to support standards-compliant H.264 AVC interworking with Microsoft's proprietary SVC implementation. Rich Media Session licenses are required on the

Expressway-C for each session to be passed through. If Microsoft Lync clients are connecting back to the network via a Microsoft Edge server, Expressway-E is required because it provides traversal using relays around Network Address Translation (NAT) (TURN) services to Lync on behalf of the Cisco receiving endpoints.

Applications

Applications available for end users are numerous. However, the applications that apply here are those mentioned in the video architecture. Specifically, these are Cisco Prime Collaboration and Cisco TelePresence Management Suite (TMS).

Cisco Prime Collaboration is a suite of applications that allow provisioning, deployment, monitoring, management, and measurement of collaboration-related metrics. With Collaboration System Release (CSR) 10.x, Cisco has begun including the Cisco Prime Collaboration Standard suite of applications (for the first cluster) at no additional cost. This includes Prime Collaboration Deployment (PCD), Prime Collaboration Provisioning (PCP), and Prime Collaboration Assurance (PCA). An upgrade is available to Prime Collaboration Advanced, which adds additional functionality to PCP and PCA while adding the Prime Collaboration Analytics module.

PCD is a migration/upgrade assistant module that provides for rapid installation and maintenance of CUCM and TelePresence components. It can provide a one-jump path for CUCM migration from very old versions to the latest version. It also assists in making the needed changes when CUCM IP address changes need to be made. It makes the needed changes throughout the cluster.

PCP is a provisioning tool that allows the creation of business rules and work flows that allow for zero-touch deployment of new users, their endpoints, clients, and voice mailboxes. When configured to sync with Active Directory (AD), PCP detects new users. It imports them into the database and provisions all the configured services for a user of that type and in that location. PCP can also replace the use of the CUCM Administration page for day-to-day move/add/change or even troubleshooting. It all comes down to work flows and the desired degree of granularity.

PCA is the monitoring, troubleshooting, and reporting module of the Prime Collaboration suite. It keeps constant track of the processes, services, call quality, and so on, just as a traditional network management suite might do. However, it is monitoring metrics such as jitter, mean opinion score (MoS), and more for voice and video calls.

TMS is a server application meant to perform provisioning, configuration, directory/phonebook functions, conference scheduling and control, endpoint/infrastructure management, and reporting for video endpoints. TMS is also used in scheduling conference rooms, allocating resources, managing CMRs, and more. It integrates with Microsoft AD and with Lotus Notes for directory and phonebook functionality. TMS also has a suite extension (TMSXE) specifically for Microsoft Outlook. This allows the creation of meetings/conference right from the Microsoft Outlook calendar page. The TMSXE module replicates calendars between TMS and Microsoft Exchange to keep track of room resources.

Summary

Video is indeed the new dial tone. Video technologies are seeing expansive growth on all fronts, be it consumer, personal, desktop, immersive, conferencing, B2B, or any other of the implementation types you might think of. It is becoming a way of life for a large percentage of the world's population. People are simply coming to expect to be able to make eye contact in any conversation regardless of device, distance, or circumstance.

The *Cisco Preferred Architecture for Video* guide details the basics of the architectures and what is needed to implement the capabilities discussed both in that document and in this book. This chapter addressed only the high-level video architecture and its core constituent components. It is highly recommended that anyone seeking a collaboration certification be familiar with the *Cisco Preferred Architecture* documents and the architectures they describe for the certification pursued.

Exam Preparation Tasks

This chapter provided an overview of the architecture and components contained in the core Cisco video architecture. The information presented here is not included in the exam blueprint. Therefore, it is unlikely that you will encounter it on the exam itself. However, the information presented in this chapter is part of a prescriptive best practice for video architecture. It is necessary information for deploying and managing Cisco video solutions.

This chapter covers the following topics:

- **Legacy Digital Media Architecture:** This section provides an overview of the evolution of digital media as a viable form of content delivery over recent decades.
- **Cisco Digital Media Suite:** This section discusses the Cisco Digital Media Suite solution, including high-level architecture and the individual components therein.
- **Capture Transform Share:** This section briefly overviews the content capture, transcoding, and publication using the DMS architecture, along with optimization capabilities.

CHAPTER 2

Cisco Digital Media and Content Delivery

This chapter provides an overview of the Cisco Digital Media Suite (DMS) solution. DMS is a video content creation, editing, transformation, and delivery architecture intended for use in a variety of manners, including education, sport stadiums, restaurant menus, staff training, and as many other uses that a moderately active imagination might contrive.

Every question deserves an answer. The age old question "why?" comes to mind when businesses and educational institutions are first presented with DMS as a potentially useful and valuable architecture. In addressing that simple question, it is necessary to understand, at least in part, the roots of the technology. With that in mind, a small discussion of history is in order, followed by a more lengthy discussion of the DMS solution and its constituent components.

Like many architectural solutions, DMS consists of a number of software and hardware components, each dependent on one another. They, in turn, make use of the underlying network and collaboration infrastructure. As the name implies, DMS is a video-based solution. As such, its traffic must be properly protected and prioritized throughout the network. A well-designed quality of service (QoS) deployment is critical to the success of any video implementation. Although QoS is beyond the scope of this chapter, it is well worth exploring and understanding. For more information on QoS, check out the following sites:

- **Cisco Quality of Service:** http://www.cisco.com/c/en/us/products/ios-nx-os-software/quality-of-service-qos/index.html
- **Enterprise Medianet Quality of Service Design Guide:** http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 2-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 2-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Legacy Digital Media Architecture	1–2
Cisco Digital Media Suite	3–6
Capture Transform Share	7–8

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. By what means was content distribution accomplished in legacy architecture?
   - **a.** Dynamic distribution using network-based architecture
   - **b.** Manual distribution
   - **c.** Proprietary distribution methodologies
   - **d.** Distribution via standards-based protocols
2. In legacy architecture, early content portals were constructed using what resource?
   - **a.** Intranet resources including internal servers, simple web pages, and wiki pages
   - **b.** Internet resources including hosted servers and network services
   - **c.** Digital media architecture solutions
   - **d.** Multicast network protocol capabilities
3. Which Cisco DMS component is used for content recording?
   - **a.** Cisco Cast
   - **b.** Cisco TCS
   - **c.** Cisco DMM
   - **d.** Cisco DMP
4. Which of the following Cisco DMS components is used as a centralized application for managing, scheduling, and publishing content?
   - **a.** Cisco TCS
   - **b.** Cisco DMM
   - **c.** Cisco Cast
   - **d.** Cisco DMP

5. Which Cisco DMS component is used in transcoding recorded media content?

   a. Cisco MXE
   b. Cisco Cast
   c. Cisco DMP
   d. Cisco TCS

6. Which Cisco DMS component is used in controlling playback of digital media?

   a. Cisco TCS
   b. Cisco Cast
   c. Cisco DMP
   d. Cisco DMM

7. Among the services offered by the Cisco Capture Transform Share solution is which of the following?

   a. Videoconferencing
   b. Video on demand and streaming
   c. WAN optimization
   d. Audio conferencing

8. ECDS is a solution that provides which of the following benefits?

   a. Video on demand capabilities
   b. Audio conference resources
   c. Content distribution management
   d. WAN optimization

Foundation Topics

Legacy Digital Media Architecture

Early implementations of what evolved into digital media systems were largely proprietary systems meant to provide surveillance capabilities. Initial systems were watch-only systems; they lacked any capability to record and store the images being collected. This meant that someone had to be physically watching the screens at all times. As the technologies advanced, recording capabilities for audio and video started to be implemented and used. These systems were adapted for use in delivering content to televisions stationed throughout office buildings, plants, and so on. This could be used to deliver morning news relevant to the business, announcements, and so on.

These systems were not attached to any external content provider, of course. All content to be presented was largely created and sourced by the entity owning the system. The "closed-circuit television" essentially signifies that the content is being sent to only a very limited set of endpoints, typically over physical media such as coaxial cable. It is the opposite of "broadcast television," which is meant to be openly provided to all capable endpoints via over-the-air broadcast.

Over time, recording capabilities evolved from reel-to-reel systems to the videocassette recorder (VCR) and then on to network-based storage capabilities. These network-based capabilities were often server-based solutions that would store content on local hard disks then push it out across a private network to proprietary display systems.

With the coming of applications such as Microsoft PowerPoint and other slide-show-capable software packages, digital signage became a viable capability. These architectures were typically built upon PC-based platforms. Those PCs would be network attached in order to provide remote management and content access. They would also provide the interface to keyboard, mouse, and monitor to make local tweaks to and display the created content.

The PC-based architecture has a number of significant drawbacks that really prevented its widespread use for dedicated digital signage. The cost of PC hardware, certainly, was one significant limiting factor. System administration difficulties, software costs, high power consumption, lack of failover/redundancy capabilities, and security (both physical and software related) obstacles made these solutions challenging, at best. In addition to these, the fact that many early solutions were proprietary meant that there could only be one source of content in specific formats for the solution. The lack of standards-compliant media was a huge challenge in attempting to make use of this kind of technology.

The fact that many systems were closed and proprietary is no surprise. Innovation waits for no one. These types of systems were needed by businesses for a number of reasons. And, they were needed right now. The business world had no time to wait for the battles to be won and lost in order to implement the systems they needed for security, content hosting, and content delivery. Where there is a need, there is going to be someone smart enough to meet it and capitalize on it.

Cisco has done much of that type of innovation over the three decades of its existence. Technologies such as InterSwitch Link (ISL) for LAN Trunking, Cisco Discovery Protocol (CDP), Cisco Power over Ethernet (Cisco PoE), and Skinny Signaling Protocol (SCCP) are big examples of that kind of innovation. No standard existed to fill the needs demanded by businesses. So, Cisco created a temporary solution while the relevant standards were being ratified and put in place. Once the respective standards became a reality and ready for prime time, Cisco instituted a technology migration to those standards. ISL gave way to 802.1Q. CDP has begun a transition to Link Layer Discovery Protocol (LLDP). Cisco PoE has become 802.1af/802.1ac/801.at PoE. SCCP is giving way to Session Initiation Protocol (SIP) now that feature parity has become a reality between the two.

Streaming Video

Providing access to streaming video in legacy environments was similarly fraught with challenges. Again, the problem largely goes back to proprietary formats and the absence of viable standards in video creation, encoding, transport, and delivery. During this time in the evolutionary stage of video streaming, the world was still largely server-based, rather than network-based. So, in the minds of many, servers *were* the network. The media and protocols used in making the servers communicate was largely irrelevant. No one single protocol had yet won the day, so to speak. Broadcast-based protocols, such as Novell's Internetwork Packet eXchange (IPX) and Apple's AppleTalk, were still prevalent in the majority of network architectures. TCP/IP was still a relative novelty in the view of many (non-UNIX) server administrators.

At the same time, Ethernet had a number of available flavors and competing technologies. 10BASE2 (thin coaxial cable), 10BASE5 (thick coaxial cable), and 10BASE-T (twisted pair) were all in widespread use as transmission media. IBM's Token Ring (at 4 Mbps or 16 Mbps) technology still had a significant foothold in the realm as well. Eventually, 10BASE-T won out over its coaxial cable-based cousins, and the battle came down to 10BASE-T Ethernet versus Token Ring. Ethernet eventually won that battle as well. But, it is worth keeping in mind that the technologies in use in the 1990s were a wild mix of Layer 1, Layer 2, and Layer 3 protocols as numerous communications methodologies fought for survival.

Today, there is one prevalent Layer 1 infrastructure for the local-area network (LAN); a similarly prevalent Layer 2 protocol infrastructure; one prevalent Layer 3 protocol; and a wide array of standards focused on communication, audio encoding/transmission, video encoding/transmission, and much more beyond that. The video battle still rages to a large degree, of course. But, it too will be settled in due time.

With all the chaos in the industry, content distribution was almost entirely manual. That is, the content had to be pushed by an administrator to a server somewhere, which is then made accessible to the PC end stations actually presenting the content. In many architectures, administrators were required to manually push the content to each local PC. It all came down to just how network aware the proprietary application in use happened to be. The use of web-based services with audio, video, and other content overlay is quite new on the scene.

IPTV

Large corporations were able to make use of streaming architectures within a campus environment by leveraging LAN-attached video encoders that were capable of leveraging IP-based streaming. The use of multicast technologies became a prevalent delivery mechanism during this time. Content came from a number of sources, including VCR/DVD, satellite, cable TV, and custom content recorded via video camera either at a company-owned studio or simply in someone's office. All these content sources could be pushed through a video encoder and onto the IP network. These IP Television (IPTV) feeds could reach the PC-based endpoints or proprietary display systems deployed throughout the campus. However, these feeds could not typically be easily stored or archived, nor could they typically be deployed in a mixed-vendor endpoint environment. This was the case even once standards-compliant streaming protocols, formats, and clients were in play.

Content Portals

In the pre-YouTube world, video distribution technologies presented more challenges than solutions, it seems. During the early evolutionary phases of content distribution technologies, ease of use was not all that high on the list. The proper use of video still required an IT personnel resource. Those user-facing tools that were available were somewhat less than intuitive. As the concept of the intranet came about, network administrators began to push more and more of the capabilities out to the user community. In most cases, this amounted to a simple web page format or a wiki-type blog format that presented links to the video files and hopefully some kind of description of the file content. As the user clicked each link, the files could be accessed and downloaded. This was usually accomplished via Common Internet File System (CIFS) or File Transfer Protocol (FTP) to deliver the file to the user's local PC. There was no means of simply embedding the video into the web page to be streamed from a central location. Resources were largely decentralized at this point.

Once downloaded, a client installed on the desktop could then be used to play each file individually. It was not unusual for a separate desktop client to be needed for each type of video format to be played.

Although the use of intranet services and wikis did offer a more streamlined means of providing content, it did not allow users to share content. In many cases, they were not allowed to upload their own content either. Each server held a different library of content (and, therefore, had to be accessed independently). This limits user interactivity, sharing, and content upload.

In today's world, content is content, and anyone can create, upload, share, and distribute it. There are obvious needs for security and protection of confidential information, of course. Those security mechanisms are certainly in place. User interfaces for these content portals are intuitive and support a wide range of software clients and hardware platforms, both static and mobile. These services are intended to provide anytime, anywhere, any device support for all content relevant to the business.

Cisco Digital Media Suite

In DMS, Cisco provides a comprehensive set of tools that enable companies to create flexible, scalable, and easily accessible content for end users, departments, peers, customers, and more. DMS offers an all-in-one solution for webcasting, video sharing, digital signage, and IPTV applications. Making the integration of digital media into the day-to-day business flow enhances communication and changes the way we collaborate and interact with our peers, colleagues, and others.

Like any other architecture, DMS includes a number of modular components. This modularity allows the creation of a custom-tailored solution based on the business needs at the time of deployment and the ability to grow, and add additional modules, as desired. The subsystems of the DMS solution are as follows:

- **Cisco Digital Signs:** Digital signage subsystem that dynamically delivers content to be displayed
- **Cisco Cast:** IPTV application that allows on-demand delivery of content
- **Cisco Show and Share:** Enables users to create live and on-demand content using social media aspects such as tagging, commenting, and rating

Each of these subsystems is discussed in later in this chapter. All the applications in the Cisco DMS solution work with the Cisco Digital Media Manager (DMM). DMM is a centralized web-based management portal through which all products can be administered. The DMM is also used in managing, scheduling, and publishing digital media content. Figure 2-1 shows the core components of the Cisco DMS solution.

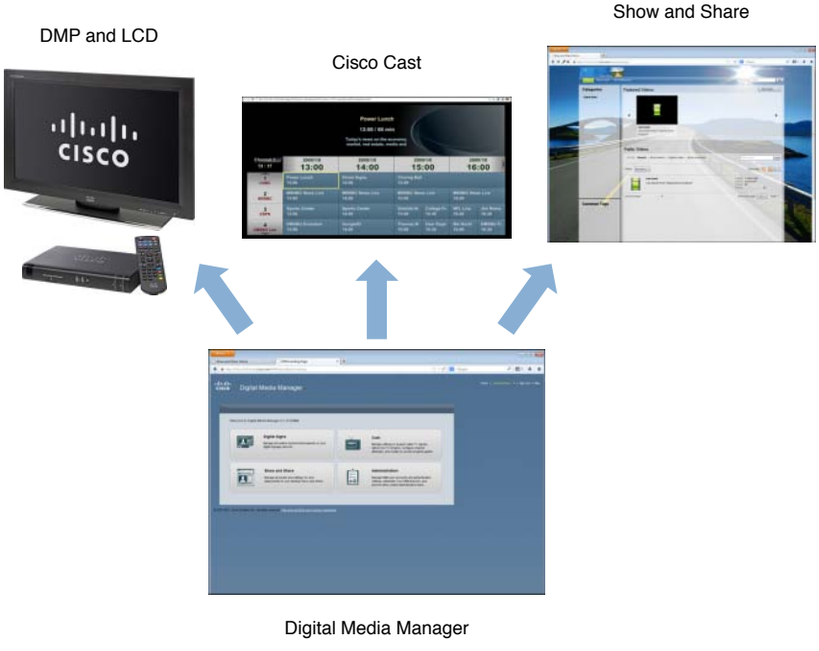


Figure 2-1 *Cisco Digital Media Suite Components*

As content is created, it can be distributed via the DMM and autoplayed or selected via Cisco Cast (think IPTV Guide) by local personnel using a remote control. A Cisco Digital Media Player (DMP) resides at each endpoint to receive the content and control the local display.

Each subsystem uses the same underlying architectural components. That is, they use the Collaboration infrastructure for call control, provisioning, resource coordination, scheduling, and so on, along with digital media specific services, including the following:

- Cisco TelePresence Content Server (TCS)
- Cisco Digital Media Manager (DMM)
- Cisco Multimedia Experience Engine (MXE)
- Cisco Digital Media Players (DMP)

Each of these components plays an important role in the overall solution, although not all are required for every individual use case. It all comes down to the desired functionality and how, and by whom, the system will be used.

DMS Components

The overall DMS portfolio consists of a number of differing facets. Each facet has a significant impact on the overall solution. As mentioned, DMS is a modular solution with a large number of potential use cases. It is common to see it used in training venues such as Cisco Live!, classrooms, or businesses wanting to train employees. It is far from a one-size-fits-all type of solution. The core pieces are the same. However, there are changes/augmentations for scalability and geographic needs.

Cisco TCS

Content can be sourced from nearly anywhere and used with the DMS solution. It can be created in a studio, conference room, office, or cubicle. There is no real limit to what can be created and pushed to the digital signage displays. The most common way content is recorded involves the use of a video camera and a Cisco TelePresence Content Server (TCS). TCS is simply a server, be it virtual or physical, dedicated to video recording and multimedia presentation for live and on-demand access. The TCS administrator can create recording aliases for content creators. To initiate a recording, simply place a video call to the alias. TCS can be scheduled as a resource via Cisco TelePresence Management System (TMS) or used on an ad hoc basis simply by adding the TCS as an attendee of a videoconference. The recording will include not only the participants, but also any secondary content shared into the conference. Any standards-compliant endpoint can participate. When the video call is disconnected, the recording stops. Then, the magic can begin. Workflow templates can be created by the administrator or by content creators; these templates will take the recorded content and transcode it into various video formats (and layouts) to optimize playback on various types of devices. Figure 2-2 shows an example of the layout template options.

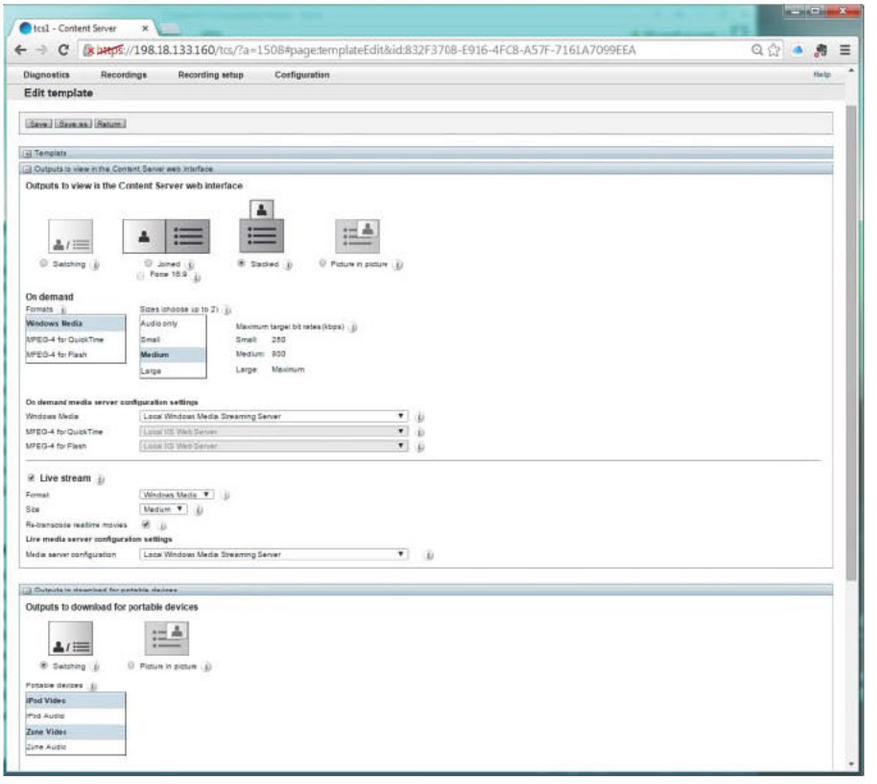


Figure 2-2 *TCS Layout Template*

Figure 2-2 shows configured output formats and layouts. Each is optimized for the type of device on which it is meant to be played and converted to the respective format for that device. Also in the template are options for both on-demand and live streaming format options.

Cisco Digital Media Manager

Key Topic

All DMS applications use the DMM as a common management platform. DMM is a web-based application that can manage, schedule, and publish content. Media and messaging are sent to the DMPs at the endpoints. The endpoints have little real control over presented content. DMM admins control what is shown and when it is presented to end users. The content can consist of live or recorded messaging or media. It can be surrounded by flash-based content as well to provide for customization. Content can be created using the Cisco Digital Media Designer (DMD) and can control when content is presented. This content can be managed, scheduled (for instant or future deployment), and published via this portal. It allows the creation of content playlists for both Digital Signs and Show and Share. The DMM also allows reporting on content playback/video usage. Figure 2-3 shows the home page of the DMM.

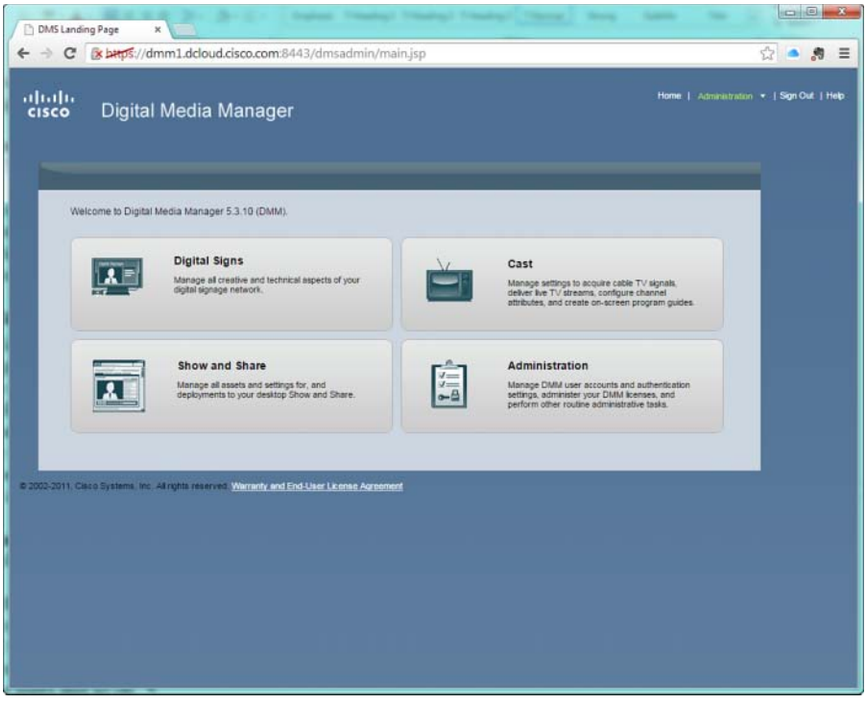


Figure 2-3 *DMM Home Page*

The DMM is the primary management interface for the Digital Signs, Show and Share, Cast, and administration of the DMM server itself. Clicking the **Administration** tile on the home page brings you to the Dashboard. The Dashboard provides a summary of DMPs in inventory, Show and Share server status, in addition to failover, clustering, and so on. Figure 2-4 shows the DMM Dashboard page.

Along the top row of the page are additional tabs for configuration of the system and its controlled subsystems. Users can be assigned to groups and roles specific to their function, be it admin, read-only, digital signage users, and so on. This administration portal is the heart of the DMS solution. It is where configuration and troubleshooting take place, services are stopped and started, licensing is applied, and so on. If there should happen to be some failure with the DMM, the DMP functionality would not be impacted.

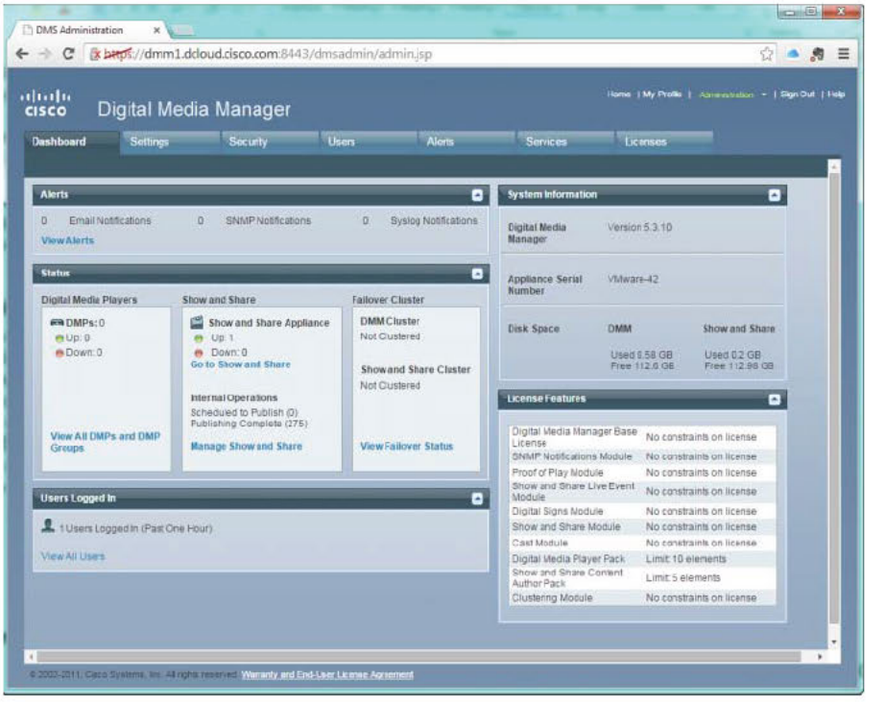


Figure 2-4 *DMM Dashboard*

Cisco Multimedia Experience Engine

Key Topic

The Cisco Multimedia Experience Engine (MXE) provides any-to-any media transformation for recorded and live content. It performs both transcoding and transrating. The previous section on Cisco TCS briefly touched on the concept of a workflow. The template, created in TCS, which specifies output video formats and layouts, is made available to content authors for selection on a per-device basis. The recorded video is passed to the MXE for conversion to the specified formats. This can be done manually or via the automated workflow mentioned earlier. The content can be adapted from nearly any format, proprietary or otherwise, and converted to any other format. It can handle audio-only, standard definition (SD), and high-definition (HD) inputs. It can also perform color correction, cropping, scaling, and more. The output media can then be viewed on a wide array of devices/applications. As new formats are introduced over time, they can be added to the MXE through system upgrades.

As mentioned, the process is easily automated. If the content was acquired in some manner other than capture via TCS or other aspect of the DMS solution, it can be manually pushed through the MXE. Figure 2-5 shows the MXE video selection page.

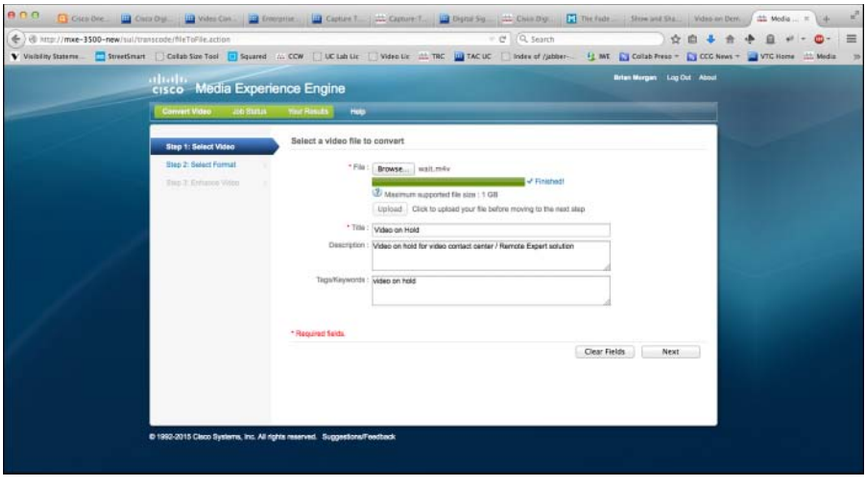


Figure 2-5 *MXE Manual Video Upload*

The process is rather straightforward. The file is uploaded via the **Browse** button. Once uploaded, a title is given to the video. Optionally, a description and tags can be added followed by a click of the **Next** button. With that done, the output formats need to be selected. Figure 2-6 shows the output format selection page.

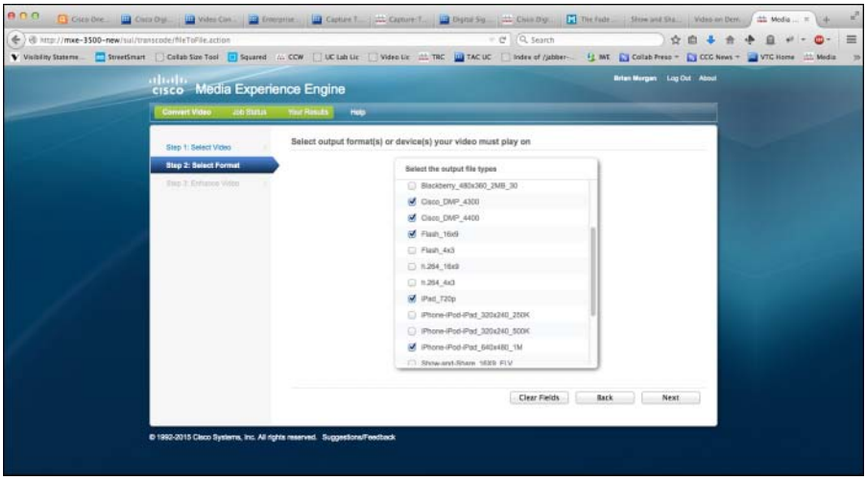


Figure 2-6 *MXE Output Format Selection*

Numerous formats are available for the output video. What is shown in the figure is only a subset of the available options. Once you select the desired output formats and click the **Next** button, additional enhancements become available. Figure 2-7 shows the options available to enhance the video.

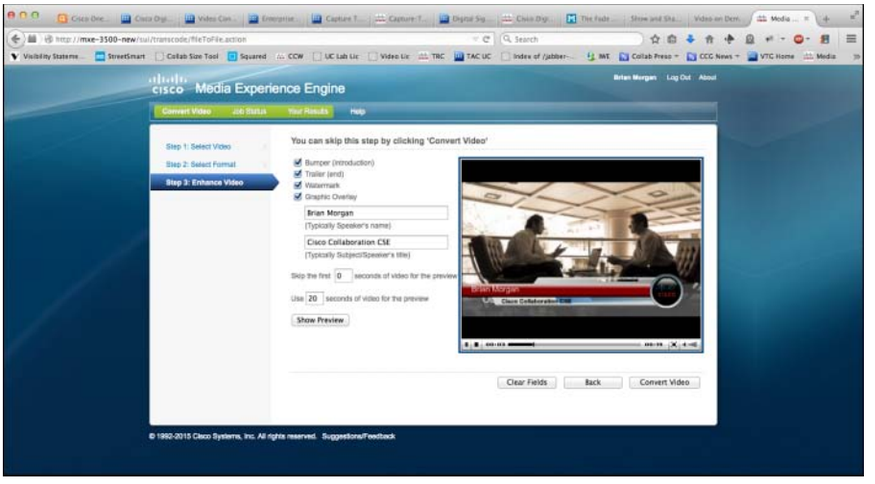


Figure 2-7 *MXE Video Enhancement Features*

As the video is processed, you can add bumpers, trailers, watermarks, and graphic overlays. Once the video is selected and configured, you can preview the video and make changes if so desired. After all options are satisfactorily chosen, you can convert the video into the selected formats. Figure 2-8 shows the job status page.

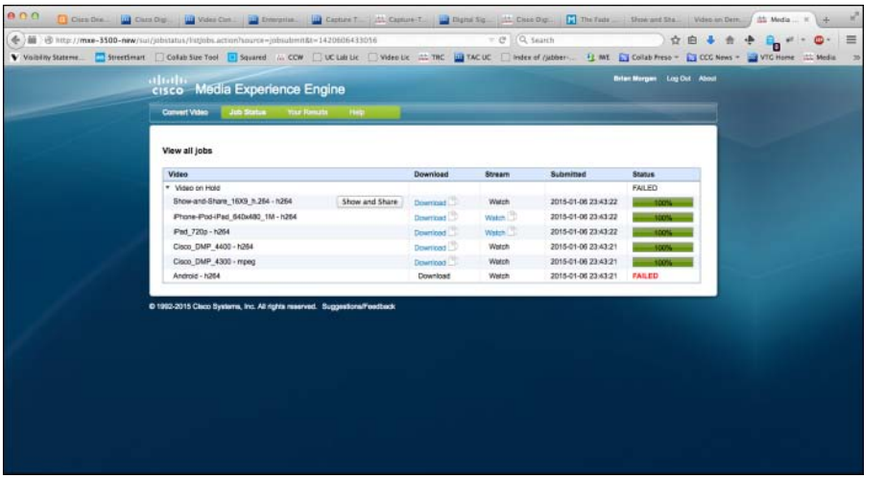


Figure 2-8 *Video Conversion Job Status*

The format conversions take place in tandem on the MXE. Each format will have a submission date and time and a status. When each one completes, a link becomes available to download it or stream it, as permitted by the format. Also, as each conversion completes, an

e-mail is sent to the user with details about the conversion, its status, and a link to download the newly created file. Show and Share formats have an additional button added to them that allows the video to be uploaded to the Show and Share server with a single click.

Aside from video format conversion, the MXE also provides Cisco Pulse Analytics. Pulse Analytics provides a means of identifying speakers in the video and creates a searchable transcript of what is said in the video. This allows viewers to search for specific speakers, content, and keywords within individual videos.

Digital Media Players

DMPs are small network-based devices that control display and playback of digital media. The content played may be web based, streaming from a site on the public Internet such as YouTube. It may also be original/custom recorded content, live streaming content, or any combination thereof. The DMP can be a standalone device. It can be configured locally rather than driven by the DMM. For a small number of devices with relatively static content, this may be an option. However, for larger numbers of devices or a requirement for dynamic, scalable content, the DMM will be of immense value.

At present, there are four models of DMPs in Cisco's portfolio: 4400 DMP, 4310 DMP, Edge 300 DMP, and Edge 340 DMP. The 4400 and 4310 are the older of the models from an evolutionary perspective.

The 4400 has a 1.5-GHz single-core processor and 1-GB DDR2 RAM. Its onboard storage consists of a 4 GB compact flash card. It does have wireless capabilities, supporting only 802.11b/g radios. It has two USB ports as well.

The 4310 has a 667-MHz single-core processor and 512-MB RAM. It does have 32 GB of onboard storage and has been given firmware updates that have enabled HTML5 content, updated video codec support, and the use of 3M and ELO IntelliTouch+ screens. These are touchscreens attached to the DMP to provide a more interactive user experience.

The Edge 300 model has a 1.2-GHz processor and 2-GB RAM. Its onboard storage, however, is only 4 GB of flash memory. In addition to support for touchscreens, the 300 has four 10/100 Fast Ethernet downlink ports in addition to the uplink port. It also has Bluetooth 4.0, WiFi (b/g/n AP or client mode), four USB ports, and built-in graphics acceleration.

The Edge 340 has a 1.6-GHz dual-core processor and 2-GB DDR3 RAM. It has a 32-GB solid-state drive (SSD) built in and an SD extension slot. Like its peer, the 340 can operate in wired or wireless environments. In wireless deployments, it can act as the AP or a client (a/b/g/n dual-band radio support). It has four USB 2.0 ports and supports Bluetooth v4.0. Unlike the 300, the 340 has no Ethernet downlink ports. The 340 is also compatible with 802.3af Power over Ethernet (PoE) and 802.3at PoE+. There is also an option to purchase the 340 without wireless network or Bluetooth support. Table 2-2 shows a summary of the Cisco DMP models and their differences.

Table 2-2 Cisco DMP Model Summary

	4400G	4310	300	340
Processor	1.5-GHz single core	667-MHz single core	1.2-GHz single core	1.6-GHz dual core
Memory	1 GB	512 MB	2 GB	2 GB
Storage	4 GB compact flash	32 GB on-board	4 GB Flash	32 GB SSD and SD Port
USB Ports	2	2	4	4
Ethernet	10/100/1000	10/100	1x 10/100/1000 uplink, 4x 10/100 downlinks	10/100/1000
Wireless	802.11 b/g	N/A	802.11 b/g/n	802.11 a/b/g/n
PoE	—	802.3af	—	802.3af

Device control between DMM and the DMP is HTTP based. The DMM uses TCP port 7777 to connect to the DMP device. Other connectivity (FTP, CIFS, and so on) may be incorporated as desired by the administrator based on the content to be presented and its source. The DMP playout architecture includes the following:

- **Live content:** All live streaming content, prerecorded content, and so on streamed through an encoder. This content uses User Datagram Protocol (UDP) for transmission.
- **Media storage and streaming:** Video content or media provided via third-party sources or external servers via HTTP, RTP, RTSP or UDP.

Note Live streaming via Real-Time Streaming Protocol (RTSP) does not support what is known as trick mode. That is, it does not support pause, fast-forward, or rewind features during video playback. It only supports start/stop functions.

- **Content and web:** DMP 4400 series can play HTTP content using a web page. The DMP 4300 series does not support HTTP playback.
- **CIFS server:** When you use Cisco Wide Area Application Services (WAAS), the DMP is instructed to use the CIFS protocol to mount/unmounts a network share such as a Microsoft Windows shared folder.

Cisco Digital Signs

Key Topic

Now that all the pieces of the architecture have been discussed, the modules can be put into place. As implied by the title, this section deals with technologies related to digital signage and how content is delivered and presented to the intended audience. Unlike its legacy counterpart, this implementation uses the network to provide a versatile mix of capabilities, including local content and on-demand network-based and live streaming capabilities. The content displayed on the endpoints can also be dynamic. That is, it can be altered based on a set of conditions set by business/security policies.

Cisco Digital Signs is the subsystem that deals with interactive on-premises digital signage that delivers video and application content to many displays. It provides a central management portal for management of DMP devices. It also allows control and provisioning of media content that shows on displays, in addition to when that content is shown. The content sent to the displays can consist of multiple formats, including Flash, live video, prerecorded video, and more. The layout of the displayed content can be customized using the Cisco Digital Media Designer (DMD).

The width and breadth of content possibilities is immense. Some possibilities include Stock tickers, RSS feeds, social media feeds, streaming video, video on demand, live video, custom-built applications, Flash media, and more. Content can be created or downloaded from anywhere on the Internet. The system supports more than simple digital signage. It can also support interactive services, such as on-demand concierge services, dynamic restaurant menu services, virtual dressing room services in retail stores, and countless other possible deployment options. All of this can, and likely will, include all the same services on mobile devices for customer interaction. Supported video formats, include MPEG1, MPEG2, MPEG4 (Part 2), and Windows Media 9 on both the DMP 4400 and DMP 4310 platforms. The DMP 4310 system also supports H.264 (MPEG4 Part 10) format. Figure 2-9 shows an example of content used in creating a digital concession stand menu.

Figure 2-9 *Cisco Digital Signage Providing Concession Stand Menu*

Cisco Cast

Key Topic

Cisco Cast is another component in the Cisco DMS architecture. It uses the DMP infrastructure to allow fast, convenient browsing and the viewing of digital media content via the use of a DMP remote control. It includes three essential functions: one to access video on demand, one to scroll through live channels, and one that provides a channel guide. Essentially, it puts the end user in control of what content is delivered to the DMP for display. This can include live news, financial information, sales/marketing information, entertainment (on demand, live, custom created), or corporate communications. It includes support for the use of standard video-streaming formats for both live and on-demand video content. This includes MPEG1, MPEG2, MPEG4 (Part 2), and Windows Media 9. Some DMP systems also support standards-based H.264 format.

Cisco Cast includes a tool called Cisco Cast Manager. This tool resides on the DMM. Using Cast Manager, channel line-ups can be defined and added to an onscreen program guide. This is the same type of experience typical when using the program guides provided by most cable and satellite companies today. The channels can include live content, on-demand content, and third-party content available via subscriptions. The channel line-ups of these third-party entities can also be integrated into the onscreen guide. Third

parties can be specific content provides, cable companies, satellite providers, or television syndicate channels. There really are no hard-defined limits on what can be brought into the guide or channel selection. In addition, Cast Manager allows customization of the guide to include corporate logos, color schemes, and so on.

Cisco Show and Share

Key Topic

Cisco Show and Share (SnS) provides a central web-based portal for users to access live or prerecorded videos and other shared content. These videos can be flagged for access control or allowed full public access. Essentially, SnS is a webcasting and video-sharing application. It provides a platform for authoring, publishing, and reviewing recorded video content. SnS supports a distributed server architecture to allow for greater scale in larger deployments. It also includes in-depth reporting capabilities for both video authors and system admins.

When used in conjunction with the Cisco Media Experience Engine (MXE), any video media format can be transcoded to any other video media format. In addition, the transcoded media can be formatted optimally for various common playback devices, such as smartphones, desktop computers, tablets, and so on.

SnS allows the creation of video communities. These communities could be based on common interests, membership in a group or class, or any other delineating factor. Access to recorded content can be limited to the community, an individual, or allowed for everyone. Regardless of author, editor, or viewer, video content supports tagging, commenting, and rating. This allows the best or most popular content float to the top of the stack, so to speak. Commonly used tags are shown in the portal sidebar.

Content can be archived, stored centrally, or distributed based on network infrastructure needs. Figure 2-10 shows the Show and Share portal interface.

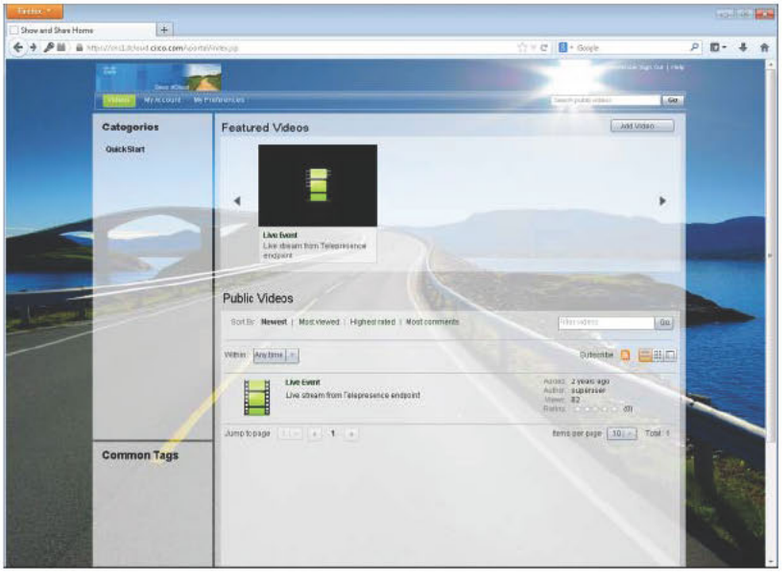


Figure 2-10 *Cisco Show and Share*

Based on size and scale, SnS can be deployed in fully on-premises, colocated, or distributed deployment models. SnS provides the following functions and features:

- Workflows for flexible authoring, publishing, and reviewing
- Multiformat file types and recording from USB cameras
- Creation of secure video communities
- Ability to enable commenting, rating, and word tagging
- Highly flexible user/group management and viewing rights
- Advanced content storage, archiving, and distribution management
- Seamless integration into the digital-content network

SnS 5.5 added a connector for Microsoft SharePoint. This allows content to be published from SharePoint to SnS. It also allows the user to surface all video from SnS directly in SharePoint. In addition to allowing for viewing of videos, it allows posting of comments directly from SharePoint.

Capture Transform Share

Capture Transform Share (CSX) is a solution more so than a product. It is the grouping of TCS, MXE, and SnS as a single architecture for content recording, transcoding/formatting, and publication. As might be expected, the solution provides for video on-demand and video-streaming services. For recording, the solution uses TCS. Recording is initiated simply by placing a call to the URI of your TCS account. To end recording, simply hang up the call. Once the call is dropped, the workflow kicks in. The recording is pushed to the MXE for transcoding to any desired format and optimized for numerous playback devices. The layout can be customized based on the type of device or media format. With that complete, the content can be pushed automatically to the SnS portal or held for approval. Additional options can be added, such as bumpers, watermarks, or Pulse Analytics.

Pulse Analytics is a speech- and voice-recognition mechanism that transcribes audio to text and identifies speakers in recorded content. Once a speaker is named, it will remember that speaker for future content publications. Once Pulse Analytics has completed processing a particular video, the text of the audio is available to those viewing the content. Spoken words are associated with individual speakers and made searchable. For example, if a professor records a biology class wherein the topic of conversation is plant life, the viewer can search on keywords such as “photosynthesis” or “cell wall” or anything else pertaining to the topic. If the keywords were spoken during the class session, each instance will be returned along with actionable links to the specific point in the discussion where the keyword occurs and who spoke the word. It provides a powerful tool for asynchronous student/teacher interaction or other non-real-time communication between presenter and viewer.

Enterprise Content Delivery System

Key Topic

Enterprise Content Delivery System (ECDS)is, as the name implies, a content delivery system. It is similar to a WAN optimization mechanism in that it allows for distributed storage and viewing of content pushed to SnS. It allows the use of existing WAN infrastructure for data and media optimization without need for bandwidth upgrades to support the additional load. ECDS can be deployed in conjunction with WAAS to provide a complete WAN optimization solution. At present, ECDS provides the following options:

- Application, e-learning, training, communications, webcasts, and digital signage delivery
- Live and video on-demand content delivery in numerous formats to large numbers of endpoints throughout an enterprise network
- Reductions in spending on streaming server and data center infrastructure for media storage
- Cost reduction through integration with media applications and optimized storage and bandwidth requirements

ECDS is an integral extension of DMS. It supports media delivery for Flash, Windows Media, Apple QuickTime, and H.264 based content. However, it includes additional components, too, as follows:

- **Service engine:** Provides edge content streaming, caching, and download of content. This includes live and video on-demand content. Also serves to provide an entry point into ECDS for live streams and allows for dynamic content retrieval using prefetch and prepositioning capabilities.
- **Service router:** Mediates requests from endpoints/clients. It is responsible for choosing the best service engine based on location and current load carried by individual service engines throughout the network.
- **Content delivery manager:** A graphical browser-based platform for management of ECDS elements. It provides a workflow-based means of automation and centralization of ECDS functions. This includes configuration, monitoring, troubleshooting, reporting, and maintenance functions.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 2-3 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 2-3 Key Topics for Chapter 2

Key Topic Element	Description	Page Number
Section	Describes DMS solution and its constituent components	22
Section	Describes the purpose and function of the TelePresence Content Server	22
Section	Describes the purpose and function of the Cisco DMM	23
Section	Describes the purpose and function of the Cisco MXE	25
Section	Describes the available DMP models and their differences	28
Section	Describes the Digital Signs subsystem of DMS	29
Section	Describes the Cisco Cast subsystem of DMS	30
Section	Describes the SnS subsystem of DMS	31
Section	Describes the ECDS solution for content delivery using WAN optimization	33

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Cisco Cast, Digital Media Designer (DMD), Digital Media Manager (DMM), Digital Media Player (DMP), Digital Media System (DMS), Digital Signs, IP Television (IPTV), Media Experience Engine (MXE), Show and Share, TelePresence Content Server

This page intentionally left blank

This chapter covers the following topics:

- **Legacy CCTV Video-Surveillance Architecture Evolution:** This section covers the evolution of video surveillance from the early CCTV monitoring systems to the IP cameras in use today.
- **Cisco Physical Security Solution:** This section covers the hardware and software products of the Cisco video-surveillance solution.
- **Cisco Video-Surveillance Components:** This section provides an overview of Cisco cameras and analytics, Cisco video-surveillance management software, and the Cisco media management and storage components.

CHAPTER 3

Cisco Video Surveillance

The Cisco CIVND 2 course is designed to cover Cisco video solutions. Most people assume that means video communications exclusively. However, Cisco has many products in other venues of video, like IP video surveillance and digital signage. To some degree, all three of these venues overlap. However, each can stand independently from the others as well.

This chapter offers a high-level overview of the solution Cisco offers in IP surveillance. The first section reviews legacy closed-circuit TV (CCTV) video-surveillance architecture and how it has evolved into what is available today. The subsequent sections cover Cisco's physical security offering, the components involved with their solution, and the architectural design of how all the different elements work together.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 3-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 3-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Legacy CCTV Video-Surveillance Architectures Evolution	1–2
Cisco Physical Security Solution	3–4
Cisco Video-Surveillance Components	6–9

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. In a traditional video-surveillance solution, what product is used to allow multiple cameras feed to display on a single monitor?

   a. CCTV
   b. Multiplexer
   c. Multicast
   d. VHS recorder

2. As the traditional video-surveillance solution evolved, what product was developed that increases the capacity of recordable storage?

   a. VHS recorder
   b. Encoders
   c. DMPs
   d. DVRs

3. What product allows for Cisco Physical Access Gateway devices to connect conventional wired sensors, along with other physical-security elements, through a converged IP network?

   a. Cisco IPICS
   b. The Cisco Physical Access Manager appliance
   c. Cisco VSM
   d. Cisco Video Surveillance Multiservices Platform

4. What Cisco product is a complete IP-based dispatch and incidence-response solution?

   a. Cisco IPICS
   b. The Cisco Physical Access Manager appliance
   c. Cisco Video Surveillance Manager
   d. Cisco Video Surveillance Multiservices Platform

5. What Cisco product is used to leverage analog video cameras in an IP video-surveillance deployment?

   a. VSM
   b. ISR
   c. Encoders
   d. Decoders

6. Which Cisco product is responsible for changing layouts that are displayed on the viewer portal stations?

   a. Cisco Video Surveillance Manager
   b. Cisco Video Media Server Software
   c. Cisco Video Operations Manager Software
   d. Cisco Video Virtual Matrix Software

7. Which Cisco product is responsible for sending video feeds to storage and viewer portal stations?

   a. Cisco VSM
   b. Cisco Video Media Server Software
   c. Cisco Video Operations Manager Software
   d. Cisco Video Virtual Matrix Software

8. Which Cisco product is responsible for interacting with the video-surveillance software through a web portal?

   a. Cisco VSM
   b. Cisco Video Media Server Software
   c. Cisco Video Operations Manager Software
   d. Cisco Video Virtual Matrix Software

9. Which Cisco product allows for up to 1 TB of storage for video-surveillance feed?

   a. Cisco Video Surveillance Multiservices Platform
   b. Cisco Integrated Services Router Generation 2
   c. NAS
   d. DAS

Foundation Topics

Legacy CCTV Video-Surveillance Architecture Evolution

In a famous scene in the movie *Indiana Jones and the Temple of Doom*, Indiana Jones triggers a chain reaction of booby traps that threaten his and his companions' lives. Although this is obvious Hollywood lore, the idea of booby traps being used to protect valuables is no new concept. They can be considered as a primitive form of surveillance that has evolved into something quite elaborate.

Video surveillance is not a new concept either. The earliest report about video cameras being used for monitoring was in 1965. These early monitoring solutions used closed-circuit television (CCTV) monitoring systems. The idea of CCTV is that a camera, drawing power from a wall outlet, also has a coaxial cable that connected it to a TV monitor. This allows for the image being captured by the camera to be displayed on the TV. If control of the camera is desired, like pan tilt zoom (PTZ), a third cable is used, called a serial cable.

Video surveillance really hit its stride when recording using tape cassettes was introduced. Magnetic tape recording devices were used as early as the 1950s, but such devices were very expensive. Judicial systems like police departments and courtrooms used this early form of monitoring, as did banks, gas stations, and other public high-risk facilities. By the 1970s, two predominant tape cassette formats took the lead in the market: Video Home System (VHS) and Betamax. Ultimately, VHS excelled in the consumer market, and Betamax went away. In retrospect, there are issues with using tape recording devices like VHS cassettes. First, the quality was so limiting that it was often hard to make out facial recognition when someone was caught on tape. Second, the recording time on a VHS cassette was limited to about 2 to 4 hours. This can be extended up to double the time length using Long Play (LP), or triple the time length using Extended Play (EP), also know as Super Long Play (SLP). By using LP or EP/SLP, the already poor quality is reduced.

Another great advancement in video surveillance was the introduction of multiplexers. Multiplexers allow for recording several cameras at a single time. In many cases, more than a dozen cameras were used at a single time. Some of the technologies around multiplexing would allow snapshot recording and motion detection recording of cameras, where they would only start recording when motion was detected. Though multiplexers brought many advantages to video monitoring, there were still many disadvantages that would need to be overcome. With a single camera, the monitor view of the camera encompassed the whole screen. With multiplexers, each camera view frame was compressed so that all camera feeds could be viewed simultaneously on the monitor. This affected the video quality even more because these smaller images could not be selected to enlarge for more detail. Figure 3-1 illustrates how a multiplexer can be used in video surveillance.

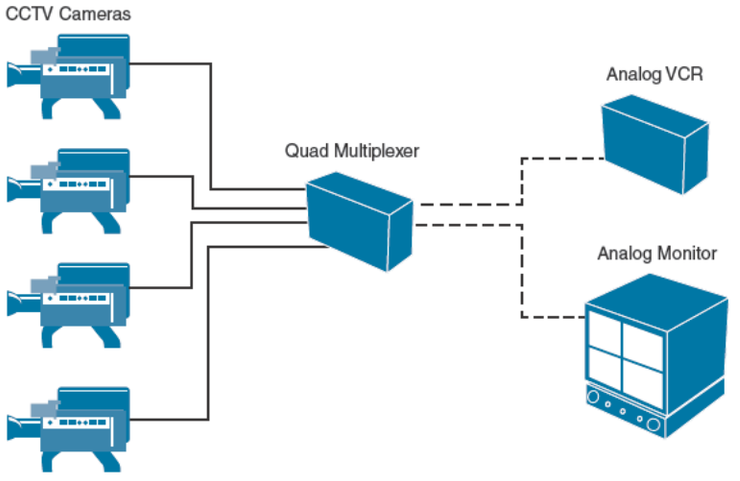


Figure 3-1 *Usage of a Multiplexer in a Video-Surveillance Solution*

It is said that invention comes from 10 percent sweat and 90 percent necessity. All the advancements leading up to this point in the evolution of video surveillance were great, revolutionary achievements for analog video monitoring. The next phase in this evolutionary process brought analog video into the digital world. One of the necessary advancements addressed the limit of tape recording devices, as well as the quality of the recorded video feed. Digital video recorders (DVRs) were introduced into video surveillance circa late 1990s. In addition to a significant increase in recorded video quality and duration of recording, there were many other advantages of using DVRs. One such advantage allowed for viewers to go back and view prerecorded video without disrupting the recording process. Another advantage is that you can select a smaller frame and enlarge it to a full-screen view. Figure 3-2 illustrates how you can use a DVR in a video-surveillance solution.

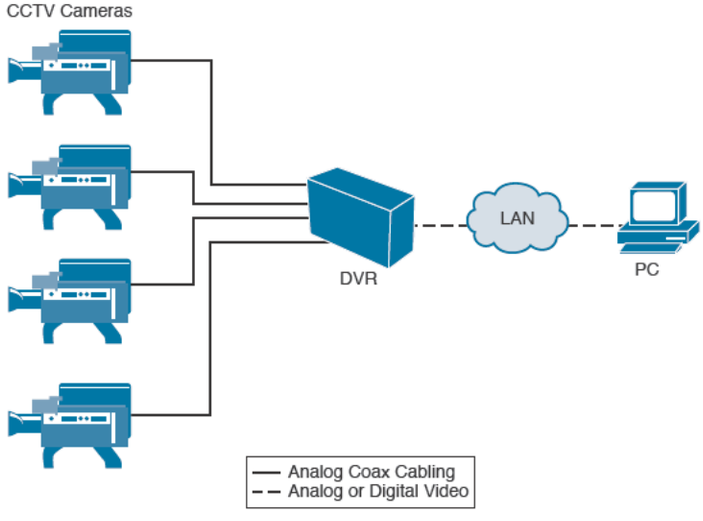


Figure 3-2 *DVR Usages in a Video-Surveillance Solution*

In the late 1990s and early 2000s, broadband and high-speed Internet were introduced. With technology taking off, and the Internet driving the information age, several more great advancements were made in the video-surveillance world. IP access to DVRs allowed viewers to access multiple locations from a central remote location. However, because analog camera had to have a physical connection to the DVR (whether directly connected or through a multiplexer), there was still a physical security issue because the DVR had to be on premises with the cameras. Encoders were introduced to video surveillance, allowing the analog signal to be converted to digital format before it was sent to the DVR. Encoders could send the digital format of the signal over an IP network to the DVR; therefore, DVRs no longer had to be stored on premises.

The introduction of IP cameras brought much advancement in the technology of video surveillance. The IP camera converted the analog video being recorded to digital format natively on the camera. This eliminated the need for encoders and traditional analog cameras. In addition, IP cameras could support Power over Ethernet (PoE), and the PTZ control of a camera could be sent over Ethernet as well. This allowed for a single cable to be run to each camera instead of the three (power, coaxial, and control) cables needed for a traditional analog camera. A modern video-surveillance solution allows for a combination of IP cameras and analog cameras with encoders to be used. Companies can still leverage their older analog cameras longer without doing an expensive tear-and-replace when upgrading their surveillance solution. As needed, those analog cameras can be upgraded to IP cameras.

Cisco Physical Security Solution

Although Cisco had already been involved in the video-surveillance market, they made a key acquisition in May 2007 of BroadWare Technologies. This acquisition brought many new and highly developed tools to Cisco's solution. With these new products available, Cisco developed a strategy based on a differentiated physical security product suit that builds on Cisco's Medianet integration. The two main components of Cisco's video-surveillance solution are hardware and software products. Hardware products include Cisco Video IP Surveillance Cameras, encoders, and physical security management and storage servers. Software products are used for monitoring video surveillance and controlling different aspects of the monitoring tools. You will learn more about these products later in this chapter. Other solution elements include the Cisco Physical Access Manager and the Cisco IP Interoperability and Collaboration System (Cisco IPICS).

The Cisco Physical Access Manager appliance is a physical intrusion-detection solution using Cisco Physical Access Gateway devices to connect conventional wired sensors, along with other physical security elements through a converged IP network. The Cisco Physical Access Manager appliance is a hardware and software solution that provides advanced configuration and management of the Cisco Physical Access Control system. The Cisco Physical Access Manager desktop client is used to define access control rules, enroll users, manage badges, and configure the Cisco Physical Access Gateway modules, among other tasks.

The Cisco IPICS is a complete IP-based dispatch and incidence-response solution with several capabilities. This solution provides an enhanced dispatch console; UHF and VHF radio interoperability; emergency first-responder notification; and integration with IP phones, cell phones, PCs, and mobile devices.

A Cisco end-to-end solution can be broken down into three categories:

- Threat detection can be categorized by the physical security elements in a surveillance solution, such as cameras, motion sensors, and access control.
- Threat monitoring is based on real-time and recorded threat-monitoring services. Such services may include door sensors and badges, fingerprint scanners or other biometric sensors, video-surveillance monitoring software, and other media management and storage components.
- The third category of the Cisco end-to-end solution is threat response. This service includes the IPICS allowing integration with existing communication devices, whether that be a Voice over IP (VoIP), public switched telephone network (PSTN), or video collaboration solution.

Components of a Cisco Digital Media Suite (DMS) could be incorporated, as well, such as PCs, Digital Media Player (DMPs), Cisco LCD Displays, and the Cisco Digital Media Manager (DMM). All three of these services work together to offer a complete and highly effective Cisco video-surveillance solution.

Cisco Video-Surveillance Components

The remainder of this chapter covers Cisco cameras and analytics, Cisco video-surveillance management software, and the Cisco media management and storage components. The Cisco video-surveillance solution can be divided into four service domains:

- Input and output devices
- Management
- Storage
- Interactive view

Input and output devices are Cisco IP cameras, analog cameras, encoders, microphones, motion sensors, and PTZ control. This chapter does not go into microphones and motion sensors in a Cisco video-surveillance solution. Management elements include features like central management of previously mentioned devices, operations like PTZ and camera switching, media control, distribution, and layout changes. Management can also determine where recorded media is to be stored. Storage involves compressing media when needed and using scalable storage solutions, whether that be locally attached storage or a network-attached storage (NAS) or storage-area network (SAN). Interactive view elements monitor endpoints such as operator view stations. It also contains distribution elements notifications and media store distribution.

Input and Output Devices

The Cisco IP cameras include standard-definition (SD) and high-definition (HD) capabilities. They communicate using IP and standards-based interfaces and protocols such as MPEG and H.264. Cisco IP surveillance cameras also include embedded security and networking, motion detection, and video analytics. As mentioned before, Cisco Medianet offers the features PoE, automated provisioning, bandwidth optimization, storage optimization, and enhanced network security. There are four series of cameras to choose from in the Cisco

solution. Each has different capabilities to cater to the various needs of the customers. Some come in a box model, and some come in the dome model. The 6000 series comes in both box and dome models. Figure 3-3 shows box and dome cameras.

Figure 3-3 *Box and Dome Cameras*

The Cisco Video Surveillance 7000 series IP cameras support a 5-megapixel lens. It is an outdoor fixed HD camera in vandal-resistant housing. This series offers excellent image quality with resolutions up to 2560x1920 and PTZ support. The Cisco Video Surveillance 6000 series IP cameras support a 2.1-megapixel lens and offers HD video capability in bullet, box, and dome models. These cameras can be used indoors or outdoor and support up to 1080p30 resolutions. The Cisco Video Surveillance 4500E series IP cameras offer true HD video at 1080p, with H.264 compression. These dome IP digital cameras are designed for superior performance in a wide variety of video-surveillance applications. The Cisco Video Surveillance 3000 series IP cameras are full-functioning HD cameras with H.264 support. These dome cameras can support resolutions up to 1280x800 at 30 frames per second. The Cisco Video Surveillance PTZ series IP cameras are available in SD or HD resolutions. Cisco PTZ IP cameras can be remotely controlled to monitor a wider area than traditional fixed cameras. Table 3-2 compares each of the camera series mentioned.

Table 3-2 Cisco Video-Surveillance Camera Features

Camera Model	Camera Type	Resolution
Cisco Video Surveillance 7000 series	5-megapixel HD IP dome cameras	Resolutions up to 2650x1920
Cisco Video Surveillance 6000 series	2.1-megapixel HD IP dome, bullet, and box cameras	1080p30
Cisco Video Surveillance 4500E series	True 1080p HD multipurpose camera	1080p30 or 720p60
Cisco Video Surveillance 3000 series	HD cameras IP dome cameras	1280x800 at 30 fps
Cisco Video Surveillance PTZ series	SD and HD IP 360 dome cameras	Up to 1080p

Another output device is the Cisco Video Surveillance Encoder. These devices use digital signal processors (DSPs) to convert analog signal from legacy analog cameras to digital format. Encoders are an optional component of the Cisco Physical Security Multiservices Platform, and the Cisco Video Surveillance Media Server Software must be installed on the server to use them. There are two cards available offering either 16 BNC connection panel or an 8 BNC connection panel on a single card. The resolution of these capture cards is D1, with motion JPEG (M-JPEG) and H.264 support. D1 resolution is 704x480, and is the highest SD resolution available in common analog-based CCTV deployments. Additional support on these encoder cards includes RS-232 for remote PTZ control of cameras.

Note that although only Cisco IP surveillance cameras are mentioned in this chapter, third-party systems are supported by the Cisco DMS solution. This includes third-party IP surveillance cameras and legacy analog cameras through encoders. Also, Cisco IP surveillance cameras are supported by third-party management software, as well.

Management

The Cisco Video Surveillance Manager Software (VSMS) is the management and control plane for the Cisco video-surveillance solution components. Cisco VSMS is a software suite that includes the Cisco Video Surveillance Operations Manager, Cisco Video Surveillance Media Server, and Cisco Video Surveillance Virtual Matrix. These software components of the VSM are the three management software solutions that are discussed in this section.

The Cisco Video Surveillance Media Server software is the core component of the network-centric Cisco video-surveillance solution. This software is responsible for the recording, storing, and streaming of video feeds. The Cisco Video Surveillance Storage System complements the Cisco Video Surveillance Media Server software. Video can be stored in direct-attached storage (DAS), NAS, and SAN storage systems. The way it works is that each IP camera or encoder sends a single video stream to the Cisco Video Surveillance Media Server. This software is responsible for simultaneously distributing live and archived video streams to viewers over an IP network. In case of multiple view requests, the software replicates the unique input video streams to multiple output streams, based on request. For archive viewing, the Cisco Video Surveillance Media Server continuously receives video from the IP camera or encoder, as configured per the archive settings. The software sends video streams to the viewer only when requested. In environments with remote branch locations, this process becomes efficient because traffic needs to traverse the network only when requested by remote viewers. Video requests and streams are delivered to the viewer by using HTTP traffic (TCP port 80) or over HTTPS (TCP port 443).

The Cisco Video Surveillance Operations Manager is the core engine for the Cisco surveillance solution. It offers centralized administration of all the Cisco video-surveillance solution components and supports Cisco video-surveillance endpoints. For security purposes, it uses authentication and access management for video feeds. Application programming interfaces (APIs) can be used for third-party integration, and third-party camera and encoder support is provided. Tools available in the Cisco Video Surveillance Operations Manager include a web-based portal that can be used to configure, manage, display, and control video from any Cisco surveillance camera or encoder. Many third-party endpoints are supported as well. Tools are available to manage multiple Cisco Video Surveillance Media

Server instances and Cisco Video Surveillance Virtual Matrix instances and users. There are also tools that control different recording options such as motion-based, schedule-based, and event-based recording. For low-bandwidth link connections, the Cisco Video Surveillance Operations Manager can perform rapid investigations using an integrated forensic search tool.

The Cisco Video Surveillance Virtual Matrix is a remotely controlled video-display application used to monitor video feeds in a command center or any monitoring environment. It enables users to control video being displayed on multiple local or remote monitors. It supports many layouts, and so operators can choose a predefined layout of cameras and push it out to the displays of all users or choose to send different users various layouts with different camera feeds. The Cisco Video Surveillance Virtual Matrix can also be integrated with other monitoring system components to automatically display video in response to user-defined event triggers. Such triggers could be from fire-monitoring systems, door sensors, and motion detectors, to name a few. Table 3-3 illustrates the three video-surveillance software components and the functions they perform.

Key Topic

Table 3-3 Video-Surveillance Software Functions

Video-Surveillance Software	Video-Surveillance Software Functions
Cisco Video Surveillance Media Server	Responsible for the recording, storing, and streaming of video feeds
Cisco Video Surveillance Operations Manager	Offers centralized administration of all the Cisco video-surveillance solution components and supports Cisco video-surveillance endpoints
Cisco Video Surveillance Virtual Matrix	Supports many layouts, and so operators can choose a predefined layout of cameras and push it out to the displays of all users or choose to send different users various layouts with different camera feeds

Storage

Many storage components can be used. Those that have already been mention include DAS, NAS, and SAN storage. The Cisco Video Surveillance Multiservices Platform has also been mentioned, and is discussed further in this section. In addition, the Cisco Integrated Services Router (ISR)-based Cisco video-surveillance elements warrant discussion.

The Cisco Video Surveillance Multiservices Platform is an easy-to-use and easy-to-deploy server suite. It offers scalable storage in a 1-RU up to a 4-RU server platform, storing up to 24 TB. As mentioned before, it supports video encoding with the optional encoder cards. There are four products in the Cisco Video Surveillance Multiservices Platform available. The virtualized applications for Unified Computing System (UCS) offer the same high security as other offering, along with other benefits of operating in a virtualized environment. The physical footprint of an organization is reduced, and the installation process is simplified, by eliminating the need for extra cabling, complexity, and power consumption. The Cisco Connected Safety and Security (CSS) UCS Platform series come in two models: the Cisco CSS UCS C220 (1-RU) and the Cisco CSS UCS C240 (2-RU). The CSS UCS Platform

series comes with a variety of choices for physical security applications. Among those are video surveillance, physical access control (1-RU only), and incident response. The next generations of Cisco Video Surveillance Multiservices Platform offerings are the Cisco Physical Security Storage System 4-RU (CPS-SS: 4-RU) and the Cisco Physical Security Storage System 4-RU-EX (CPS-SS: 4-RU-EX). This series is ideal for performing backup to disk and bulk data storage.

Cisco video-surveillance cards are also available for the Cisco Integrated Services Router Generation 2 (ISR-G2). These module cards make management of analog cameras in remote offices more efficient, while supporting an IP video-surveillance network. When the ISR-G2 routers are used with the Cisco video-surveillance cards, 1 TB of DAS storage is made available.

Key Topic

The Cisco Analog Video Gateway Module provides support for analog cameras, PTZ, alarm input, and control relay output. This module can support up to 16 analog cameras in a single card. The Cisco Analog Video Gateway Module is controlled by Cisco Video Surveillance Stream Manager. Cisco Analog Video Gateway Module encoders and decoders use the MPEG4 video compression codec, allowing for streams to be sent over the network using D1 resolutions up to 30 fps. The encoder that connects to the analog camera simultaneously records two MPEG4 streams at different resolutions. This enables viewers to observe high-quality streams, while a lower-quality recording will use less storage space.

The Cisco Video Management and Storage System Module implements the Cisco Video Surveillance Media Server and the Cisco Video Surveillance Operations Manager for the branch office. The Cisco Video Management and Storage System Module supports IP video cameras connected to the ISR through the IP network, in addition to any analog cameras connected through the Cisco Analog Video Gateway Module and most third-party cameras. Notifications can be sent from the router using e-mail messages, pages, and SMS.

Table 3-4 illustrates the two storage options discussed in this section, with their storage capacities and the type of storage available natively to the systems.

Key Topic

Table 3-4 Cisco Storage Options

Cisco Storage Device	Storage Capacity	Type of Storage available
Cisco Video Surveillance Multiservices Platform	Up to 24 TB	DAS
Cisco Integrated Services Router Generation 2	Up to 1 TB	DAS

Interactive View

The Cisco video-surveillance solution is based on service domains. The domains that have already been discussed include the VSM software suite and video-surveillance storage systems. The Cisco video-surveillance solution can integrate with other Cisco connected physical security elements such as media and threat distribution, the Cisco DMS, and Cisco's Collaboration endpoints. Other architectural domains include video input and edge analytics, sensors, PTZ camera control, and interactive output. This section takes all the elements

that have been discussed and explains the flow of media, the communication signaling paths, and interactive views that can be used in a Cisco video-surveillance solution. The two scenarios that are discussed are the Cisco Video Surveillance Operations Manager Viewer and the Cisco Video Surveillance Matrix Viewer.

When an operator is interacting with the Cisco video-surveillance software, the Cisco Video Surveillance Operations Manager software is being used through Microsoft ActiveX web browser. This traffic can use TCP port 80 (HTTP) or 443 (HTTPS). The following steps outline the process Cisco's video-surveillance software follows to change camera views:

1. Using this software, the operator can select which cameras need to be viewed on which displays and in what camera positions.
2. The Cisco Video Surveillance Operations Manager then sends a signal to the Cisco Video Surveillance Media Server requesting the video feed from the selected cameras.
3. The Cisco Video Surveillance Media Server requests video feed form the appropriate cameras.
4. The camera sends the video feed to the Cisco Video Surveillance Media Server.
5. The Cisco Video Surveillance Media Server using TCP, UDP, or multicast sends these views to the Cisco Video Surveillance Operations Manager.
6. The Cisco Video Surveillance Operations Manager updates the view on the appropriate view portal stations based on the parameters selected by the operations manager. The protocol used is based on what was requested by the Cisco Video Surveillance Operations Manager.

Note The number of video feeds that can be shown depends on the CPU, RAM, and so on of the computer. If all the feeds are displayed, some might show as thumbnails only or might even make the PC unresponsive.

If another Cisco Video Surveillance Operations Manager Viewer requests the video from the same IP camera, the Cisco Video Surveillance Media Server simply replicates the video stream as requested. No additional requests are made to the camera. Figure 3-4 illustrates the Operations Manager Viewer scenario.

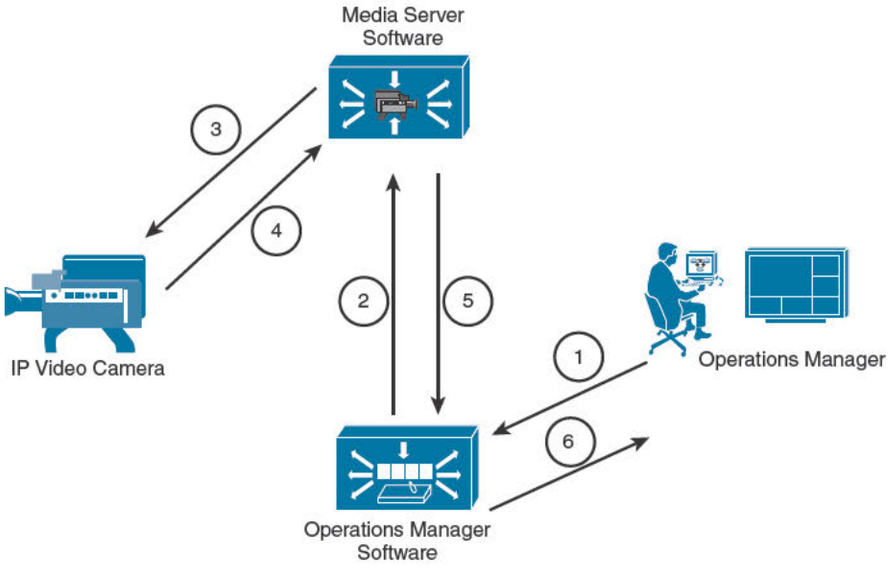


Figure 3-4 *Operations Manager Viewer Flow Scenario*

The process for switching layout views using a Cisco video-surveillance solution is similar to the previous scenario. Again, when an operator is interacting with the Cisco video-surveillance software, the Cisco Video Surveillance Operations Manager is being used. The following steps outline the process Cisco's video-surveillance software takes to change layouts and update camera views:

1. Using this software, the operator can select which layout is desired and which cameras need to be viewed within the different panes on that particular layout. That communication is sent to the Cisco Video Surveillance Operations Manager through the web portal.
2. The Cisco Video Surveillance Operations Manager then sends a signal to the Cisco Video Surveillance Virtual Matrix requesting a particular layout.
3. The Cisco Video Surveillance Virtual Matrix determines what layout and what cameras are to be used. Then the Cisco Video Surveillance Virtual Matrix sends a signal to the Cisco Video Surveillance Media Server to request video feed form the appropriate cameras.
4. The Cisco Video Surveillance Media Server requests video feed form the appropriate cameras.
5. The camera sends the video feed to the Cisco Video Surveillance Media Server.
6. The Cisco Video Surveillance Media Server sends these views to the Cisco Video Surveillance Virtual Matrix.
7. The Cisco Video Surveillance Virtual Matrix sends the communication to the operations view portal monitors directly.

The Cisco Video Surveillance Virtual Matrix sends a keepalive message to the operations view portal monitors periodically to confirm that the displays are still active. Figure 3-5 illustrates the Cisco Video Matrix Viewer scenario.

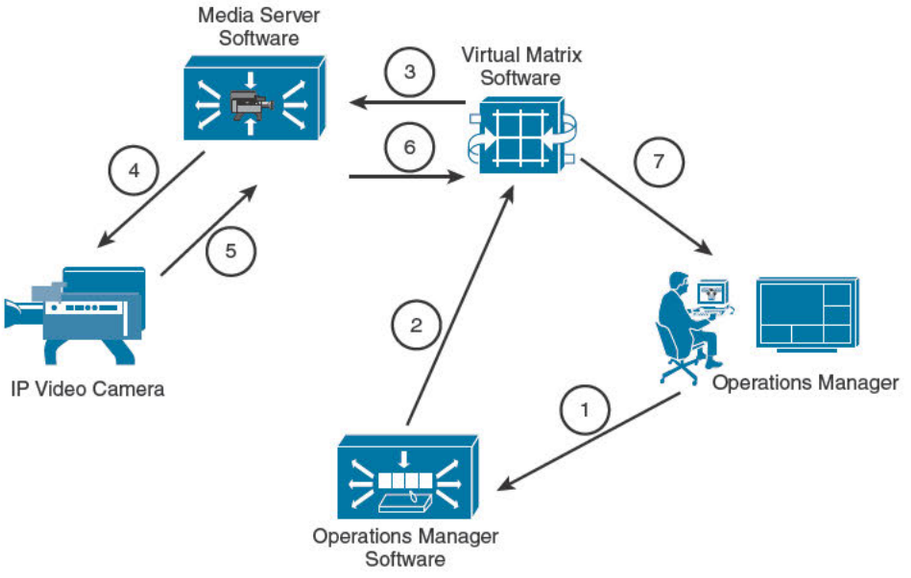


Figure 3-5 *Cisco Video Matrix Viewer Flow Scenario*

Summary

Because of greater needs, the desire for better quality, and key advancements in technology, video surveillance has evolved from its rudimentary form over several decades. From these advancements, Cisco offers a robust and secure video-surveillance solution for customers based on modern-day needs. The Cisco video-surveillance solution offers a wide assortment of IP video cameras and encoders that enable you to leverage analog camera that may already be in use. You can manage these components securely and effectively by using Cisco's VSM software suite, which includes the Cisco Video Surveillance Operations Manager, Cisco Video Surveillance Media Server, and Cisco Video Surveillance Virtual Matrix. This software platform offers integration with other components within an organization like emergency response and other secure devices incorporated into the business environment. All of this is supported on a Cisco Video Surveillance Multiservices Platform. This server basis has scalable built-in storage and can integrate with NAS and SAN storage as well. The Cisco ISR allows for remote management of remote office facilities, completing the Cisco video-surveillance solution. Memory table are provided for review of key information discussed during this chapter. Review these memory tables to ensure a solid understanding of these topics.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 3-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 3-5 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
Paragraph	Use of multiplexers and DVRs	40
Paragraph	Physical intrusion-detection solutions	42
Table 3-3	Cisco video-surveillance software functions	46
Paragraph	Cisco ISR module options	47
Table 3-4	Cisco video-surveillance storage capacity and type	47

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

CCTV, Cisco IPICS, Cisco Video Media Server, Cisco Video Operations Manager, Cisco Video Virtual Matrix, CSS UCS, DAS, DSP, DVR, EP, HD, HTTP, HTTPS, LP, multicast, NAS, PoE, PTZ, SAN, SD, SLP, TCP, UCS, UDP, unicast, VHS, VoIP, VSM

This chapter covers the following topics:

- **Legacy Videoconferencing:** This section covers the history and evolution of videoconferencing technologies and infrastructure.
- **Introducing Cisco Collaboration Solutions:** This section provides an overview of the technology categories comprising Cisco collaboration solutions.
- **Cisco Collaboration Architecture:** This section explains how these technologies work together to create a cohesive, end-to-end user experience second to none.

CHAPTER 4

Cisco Collaboration Overview

This chapter focuses on the early architectures and evolution of video-based communications and conferencing. As with the evolution of any technology, video has a reputation for being difficult and expensive. Video as a communications medium has been around for some time; however, only in the past few years has it evolved sufficiently to become a truly viable and cost-effective communications architecture solution. Video collaboration technologies have quite a formidable reputation to overcome. That reputation is one that generally casts it in a less-than-positive light.

However, that reputation is quickly being overcome as business needs continue to demand more frequent in-person meetings with colleagues, team members, customers, suppliers, students, teachers, doctors, and so on regardless of the distance and geography between them. Over the past few years, Cisco has reinvented itself from a collaboration perspective. The cost of video endpoints and architectural infrastructure has come down dramatically in a very short time. Removing cost as a barrier to entry into the world of videoconferencing has been an extreme boon for its continued expansion into the business world.

The evolutionary path has been somewhat difficult. And, as mentioned, that path has also been quite expensive, both in terms of man-hours and dollars spent implementing the technologies.

Regardless of whether the discussion is centered on audio or video, there are three essential types of conferences:

- **Instant (a.k.a ad hoc):** You're talking to one person and want to add a third person to the call.
- **Personal (a.k.a rendezvous/meet-me):** Permanent, persistent conference resource. Think of it as a personal virtual meeting room.
- **Scheduled:** Invitations are e-mailed out ahead of time and resources reserved in advance.

The underlying principle is the same regarding videoconferencing. In videoconferencing, as in audio conferencing, there must be some kind of resource to handle the call media and attendees. That is, there has to be some kind of resource, be it software or hardware, that can take in the media, mix it, and send it back out to the attendees. This resource is simply referred to as a conference bridge. This chapter focuses on the technological evolution and advance of videoconferencing.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 4-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 4-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Legacy Videoconferencing	1–3
Introducing Cisco Collaboration Solutions	4–6
Cisco Collaboration Architecture	7–9

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following transport technologies uses 23 B channels and a D channel?
   - **a.** T1 CAS
   - **b.** T1 PRI
   - **c.** E1 CAS
   - **d.** E1 PRI
2. Which of the following first provided centralized call control capabilities for H.323 video endpoints?
   - **a.** Gatekeeper
   - **b.** CUCM
   - **c.** MGCP
   - **d.** MCU
3. Which of the following provided a total usable bandwidth of 128 kbps?
   - **a.** BRI
   - **b.** T1 PRI
   - **c.** T1 CAS
   - **d.** E1 PRI

4. Which of the following are needed to facilitate a videoconference? (Select all that apply.)

   a. Endpoints
   b. Bridging resource
   c. Call control
   d. Cisco TCS

5. Customer collaboration refers primarily to which of the following?

   a. Call control solutions
   b. Conferencing solutions
   c. Contact center solutions
   d. Unified communications

6. Which of the following provides an on-premises web/audio/videoconferencing solution?

   a. Cisco WebEx Meeting Center
   b. Cisco WebEx Meetings Server
   c. Cisco WebEx Event Center
   d. Cisco WebEx Training Center

7. Which management tool is Microsoft Windows Server based and can be installed onto either a virtual or physical server operating system instance?

   a. MXE
   b. TMS
   c. VCS
   d. VTS

8. Which of the following are call control elements? (Select all that apply.)

   a. CUCM
   b. VCS
   c. Expressway
   d. TMS

9. Which of the following solutions allows for VPN-less access from mobile devices and endpoints, outside the network, to internal voice/video calling, IM/presence, voice messaging, and other UC services?

   a. Expressway
   b. TMS
   c. ASA
   d. CAC

Foundation Topics

Legacy Videoconferencing

Like many technologies, video started off quite modestly. The capabilities were largely limited to point to point and utterly absent industry standards or any real call control capabilities. As with many technologies, the base functionality was the first thing to be established, with user friendliness taking a position very far down on the list of priorities. This was the case for quite a long period of time. As user-centricity began to take the spotlight in nearly every other aspect of technology, video still remained somewhat stagnant and, sadly, difficult and expensive to use. That combination of characteristics has been the downfall of many other technologies; however, real-time video has always seemed to have a place at the core of our underlying communications goals. It has been embedded in our society as simply the way things are going to be. Every futuristic book and television show as far back as many of us can remember had some focus on video as a communications medium. Perhaps that is why it hung on long enough for the surrounding architectures to build up around it and allow it to emerge from the recesses of our imaginations as a viable means of communication.

Early Transport

Key Topic

The earliest video endpoints relied upon Integrated Switch Digital Network (ISDN) Basic Rate Interface (BRI) or Primary Rate Interface (PRI) technologies for transport. BRI circuits consist of two bearer (B) channels and a data (D) channel. Each B channel provides 64 kbps of bandwidth for a total of 128 kbps, whereas the D channel is a 16 kbps signaling channel. BRI is also known as 2B+D. PRI circuits vary in composition based, generally on geography. In the United States and Japan, T1 is used; in Europe and other geographies, E1 is used.

T1 and E1 circuits come in two general flavors: PRI and Channel Associated Signaling (CAS). T1 PRIs consist of 23 B channels and a D channel, 23B+D, whereas T1 CAS circuits consist of 24 timeslots that are time-division multiplexed (TDM). The total bandwidth of a T1 is 1.544 Mbps PRI or CAS.

The E1 is a 32-channel circuit. E1 PRIs consist of 30 B channels and a D channel, 30B+D. In a CAS E1, 30 channels are used for payload or user traffic while one channel (channel 0) is used for framing (synchronization, alarm transport, CRC, and so on) and one channel (channel 16) is used for signaling. In an E1 PRI, channel 16 is the D channel. The following table provides a summary of the available circuit types.

Type	Data Channels	Special Channels	Geography
BRI	2 x 64 kbps (B)	1 x 16 kbps (D)	Global
T1 PRI	23 x 64 kbps (B)	1 x 64 kbps (D)	North America, Japan
T1 CAS	24 x 64 kbps	— (in-band signaling)	North America, Japan
E1 PRI	30 x 64 kbps (B)	2 x 64 kbps (framing and D)	Europe, Australia, South America
E1 CAS	30 x 64 kbps	2 x 64 kbps (framing and signaling)	Europe, Australia, South America

Low-resolution endpoints commonly used three BRIs to support 320 kbps for video and 64 kbps for audio. This video stream typically used Common Interchange Format (CIF) for communications. Higher-resolution endpoints were able to make use of PRIs, be they T1 or E1. As might be expected, many of these calls, regardless of resolution, would incur long-distance or international public switched telephone network (PSTN) calling charges. This contributed immensely to the cost of the technology at the time. Figure 4-1 shows a simple example of a point-to-point video architecture.

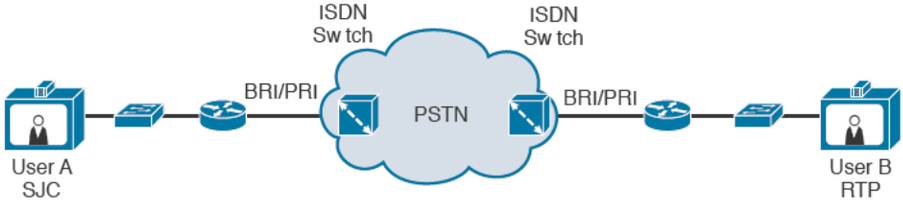


Figure 4-1 *Legacy Point-to-Point Video*

The figure shows a couple of endpoints using digital circuits for connectivity. ISDN provided the transport over which IP traffic could flow between the two endpoints. The endpoints would use IP addresses to dial one another. There was no real concept of a centralized call control element at that time. The underlying routing protocol directed the traffic to the local ISDN gateway, which would then invoke a dial-on-demand routing (DDR) call to the far-end ISDN gateway to establish a path across the network between the endpoints. With a BRI circuit, each channel has an associated phone number. To dial between the two sites, as in Figure 4-1, long-distance calling is required to make the connection. Suffice to say that it got expensive rather quickly once three BRI circuits were in use for a single cross-country video call.

IP to the Rescue

As the technological evolution progressed into the early days of Voice over IP (VoIP), the solution took a bit of a leap forward. Now that IP trunking is a reality, the usage of the ISDN circuits could be significantly reduced or eliminated altogether in favor of a wide-area network (WAN) solution. Technologies such as digital subscriber link (DSL) became widely available for both business and residential use. This was the first large leap away from ISDN in terms of both wide reachability and high bandwidth being balanced with cost-effectiveness. Through the 1990s and into the 2000s, the advent of Multiprotocol Label Switching (MPLS) networks further increased the capabilities and reach of the network by effectively eliminating the concept of hub-and-spoke networks, which are typically latency rich. MPLS provided a more cost-effective means of creating a fully meshed environment than was feasible with other WAN technologies at the time. As you might expect, excessive latency is a very bad thing in terms of voice/video quality.

Initially, all video communications were established using H.323 protocol capabilities. This is largely due to the fact that H.323 is quite similar in operation to ISDN, in terms of messaging, troubleshooting, and so on. H.320 is a general recommendation for running voice, video, and data over ISDN circuits. The PSTN side of the connection handled audio, albeit out of band.

At this point, there is still no true central call control element; however, we do finally see the advent of true conferencing as a technological possibility, even over distance. This is accomplished largely by the rapid spread of WAN technologies throughout the globe. By keeping the traffic on-net, large corporations are suddenly able to eliminate the geographic barriers that made ISDN-based calling so expensive.

A video call is generally accepted to imply a point-to-point nature. The call does not become a conference until a third endpoint is added to the call. As mentioned at the beginning of this chapter, a conference requires a bridging resource. Bridging resources can come in the form of hardware-based multipoint control units (MCUs), or they may be software-based MCU equivalent entities. Either way, there is a means of mixing the media and getting it to all participating endpoints. Many early adopters of videoconferencing technologies did eventually get around to investing in their own infrastructure. For those companies that were just not quite there financially, hosted MCU providers began popping up all over the place. A large percentage of these providers were productizing hosted best-effort MCU services and expanded reachability made possible by a brand-new transport option called the Internet.

Multipoint conferencing technologies began to rapidly evolve in terms of reachability. With the availability of both hosted and private videoconferencing resources came the need to expand the options of who could and could not attend a videoconference. These resources would need to support any combination of ISDN-based or H.323-based connections for both audio and video participants. Obviously, the need to support the use of Internet-based endpoints revealed a somewhat significant issue regarding quality of service and reliability. Figure 4-2 shows how this expanded architecture looked in terms of transport and reachability between endpoints.

In the figure, all the transport mechanisms discussed thus far are represented. Those using the Internet and WAN transport would be using H.323, whereas the PSTN-based endpoints would be making use of ISDN technologies.

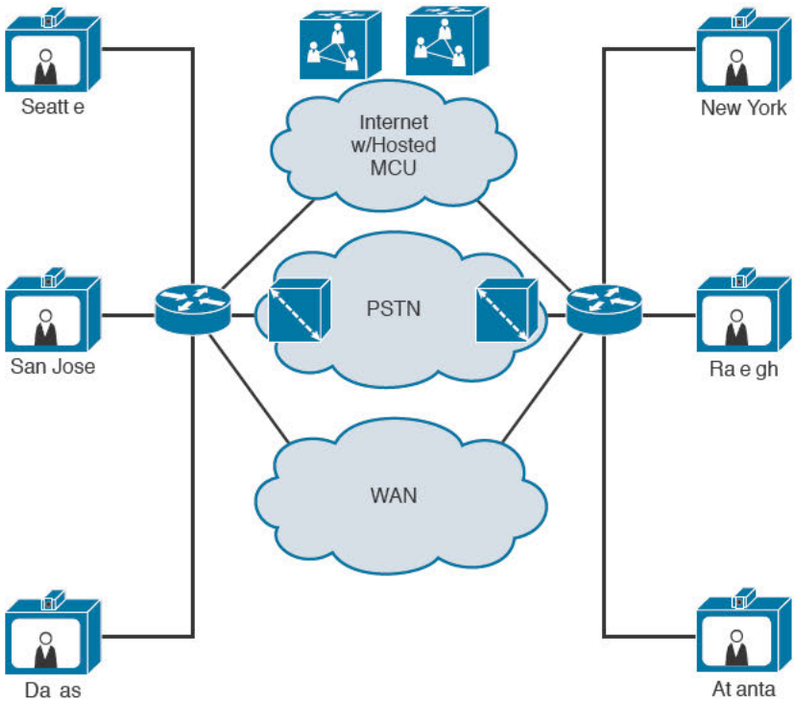


Figure 4-2 *Legacy Videoconferencing Architecture*

Early Call Control

Key Topic

Up to this point, there was no real methodology for providing a central call control element. As video infrastructure began to scale, the administration of the dial plan became more than a little cumbersome. In addition, bandwidth concerns emerged as a very real issue throughout the network. Something was needed to manage both the dial plan structure and to meet the needs of those seeking to exercise some level of call admission control (CAC). With that in mind, H.323 gatekeepers came about. The gatekeeper provides a good spectrum of control options. This includes the ability to scale immensely as well as to control calls both within sites and calls traversing the network to other sites.

Keep in mind, true quality of service (QoS) had not even begun to emerge as a network requirement for protecting high value or critical traffic. Queuing and compression methodologies were about as close as one might get to anything resembling QoS.

The gatekeeper provided an on-premises control plane to the network. It could (and still can) provide control for H.323 audio calls and video calls. In Cisco's implementation, the gatekeeper was simply a voice-capable router with a specific feature set and configuration.

Traditional private branch exchange (PBX) infrastructure provided additional connectivity options for those corporations large enough to have a significant infrastructure. If these companies were able to traverse their own PBX switching infrastructure, it became possible, even likely, that they would use their own internal PRI/BRI circuit capabilities to keep calls

on-net. Even if the calls were not able to be kept on-net all the way from end to end, they could be routed to the nearest possible point to the destination, thereby avoiding, or reducing, toll charges. Figure 4-3 shows a logical view of this type of topology.

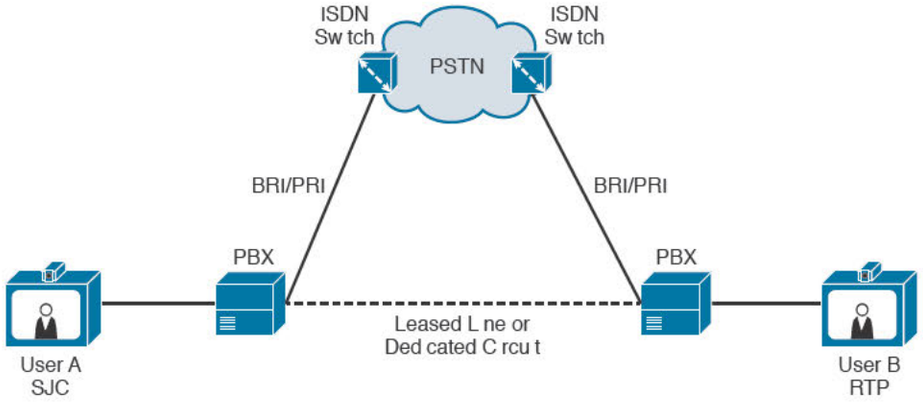


Figure 4-3 *Legacy Video Calling with PBX Infrastructure*

Then, like now, corporations needed to be able to support multiple potential solutions and technologies. The use of on-net resources coupled with off-net resources quickly spawned hybridized topologies. These topologies used a combination of PBX, PSTN, and H.323 to meet the needs of the business. This obviously added a significant degree of complexity in addition to the great flexibility it provided. Figure 4-4 shows a logical diagram of a hybrid legacy communication architecture.

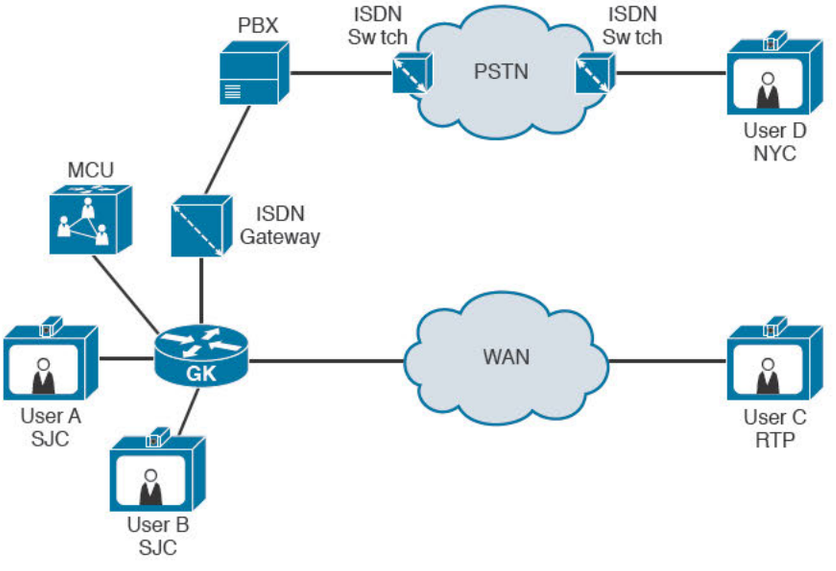


Figure 4-4 *Legacy Hybrid Video Calling Infrastructure*

In the figure, there is a distinct mix of technologies, including a gatekeeper for call control, a PBX for PSTN/ISDN connectivity, a WAN infrastructure transporting on-net video, and an MCU to provide bridging resources. The ISDN gateway is a customer premises equipment (CPE) device that provides an interworking function between the ISDN network/PBX and the IP-based endpoints, gatekeeper, and MCU.

Introducing Cisco Collaboration Solutions

Cisco collaboration solutions consist of a number of architectural components. The network provides the foundation on which the collaboration applications rely. As mentioned in Chapter 1, "Introduction to Video Communications," the Cisco Preferred Architecture includes five subsystems within the collaboration architecture.

However, from an exam perspective, the more relevant aspects of collaboration architecture include technology categories, rather than the subsystems. The technology categories include the following:

- **Unified communications:** Solution components aimed at bringing together voice, video, data, and mobile applications. This includes call control, gateways, and applications.
- **Customer collaboration:** Solution components aimed at customer interaction, such as contact center applications and voice self-service products. This typically focuses on Cisco Unified Contact Center Express (UCCX) and Cisco Unified Contact Center Enterprise (UCCE) solutions for customer interaction.
- **Conferencing:** Solution components used to enable anyplace/anytime multiparty communications with a focus on security, high quality, and content sharing. This includes audio and videoconferencing products, web conferencing applications, and conferencing management/scheduling tools.
- **Collaboration endpoints:** These are the video and telephony desktop, mobile, and software components used by end users to communicate. This includes IP Phones, collaboration desktop endpoints, Cisco TelePresence room-based and immersive endpoints, software clients, and Cisco TelePresence integrations.

Regardless of how the Cisco collaboration solution architecture is broken down, the pieces remain fairly much the same. There is a high degree of modularity in the overall solution. Many of the pieces can be mixed and matched to fit what is right for a given business or need. The underlying foundation is the call control element. Cisco Unified Communications Manager (CUCM) is the essential glue that holds the entire architecture together. The gateways are essentially extensions of the CUCM as it controls the ports through which calls will ingress and egress.

Additional flexibility in the solution is provided by the simple fact that the solution can be wholly on-premises or it can be cloud-based in the form of a hosted collaboration service (HCS). The architecture is nearly identical aside from the fact that a service provider is hosting all of the relevant pieces within their network.

In an HCS solution, the only components typically on premises are the IP Phones, collaboration endpoints, conferencing resources, and gateways. The rest of the collaboration solution components are in the provider cloud infrastructure. HCS solutions are priced based on

user count and the capabilities/features to be employed by each user. From a feature and capability standpoint, HCS solutions can offer the same capabilities as fully on-premises solutions. Customers who want to make immediate use of the business advantages offered by video solutions can benefit immensely from an HCS deployment. The turnaround on the deployment of the solution is exceedingly rapid, with significantly reduced overall capital expenditure for on-premises equipment and staff training.

Unified Communications

Key Topic

The term *unified communications* came about as a way to describe a single architecture aimed at providing a rich communications experience anytime, anywhere using any endpoint. Over the past couple of decades, the term has evolved. When Cisco first stepped into the telephony market, the Architecture for Voice, Video, and Integrated Data (AVVID) was introduced. It eventually gave way to the concepts encompassed by unified communications and collaboration. Until now, the architectures have been fragmented and isolated entities functioning largely as ships in the night. The voice infrastructure traversed its own dedicated hardware. Its network infrastructure was entirely dedicated to voice. This included dedicated leased lines, trunking resources, and more. The same is true, as has been discussed in the first section of this chapter, for video. Applications were generally one-off, proprietary pieces of software built entirely in-house. There was no common foundation on which everything could build as a single solution until the network came along. Along with the network came communication standards for transporting voice and video over TCP/IP and other technologies.

The state of the technologies has finally reached the point where a single infrastructure, a single core element, can provide the applications and services to voice and video endpoints, mobile clients, applications, and more. Call control, voice mail, conferencing, video, instant messaging (IM), mobility, presence, contact center, and security along with e-mail, calendar, and directory services integration capabilities have all converged to create a seamless communications experience regardless of device or locale.

Customer Collaboration

Cisco's customer collaboration solutions include two options at the very high level. These are Cisco Unified Contact Center Express and Cisco Unified Contact Center Enterprise. The decision to use one or the other is largely based on the number of agents desired and the degree of functionality/interaction desired with customers. UCCX can support up to 400 agents on a single virtualized server instance. For high availability (HA), a second server of equal size is deployed. UCCE allows scaling of agents up to 12,000. UCCE is a significantly more robust and feature-rich solution and is highly customizable.

Both solutions can use the Cisco Agent Desktop (CAD) or the Finesse Desktop. Finesse is a web-based agent interface that allows for greater flexibility in use, monitoring, integration with other applications, and customization.

As video architectures have become more pervasive, both UCCX and UCCE have begun to support the use of video endpoints for agents. The video contact center is a rapidly growing field of specialization within customer collaboration solutions.

Conferencing

Conferencing has expanded greatly over the years to encompass more than simply bridging phone calls together. Audio and videoconferencing architectures have become more and more feature rich, allowing companies to scale their solutions to never-before-seen capacities. The scope of possibilities has also expanded. Conferencing now requires a much wider array of service offerings, including the traditional on-premises audio and videoconferencing, but expanding to include web conferencing, application integration, cloud-based conferencing options, and hybrid solutions allowing the seamless integration of both on-premises and cloud-based conferencing resources in a single meeting. As mentioned in the chapter introduction, there are three essential types of conferences:

- Instant (or ad hoc) conferences
- Personal (or rendezvous/meet-me) conferences
- Scheduled conferences

In all three cases, the basic requirements are the same. In the context of this discussion, they require CUCM or Video Communication Server (VCS) for call control, a conference bridge resource (hardware or software based MCU), and of course the actual video endpoints participating in the conference. CUCM or the MCU bridge resource can be either on-premises or hosted (cloud-based).

The Cisco acquisition of WebEx immensely upped the standard for web/audio/videoconferencing in a cloud-based environment. Cisco WebEx includes four centers for meetings:

- **WebEx Meeting Center:** The default meeting front end for Cisco WebEx. Meeting Center allows attendees to use audio, web, and video resources for day-to-day meetings. Content can be shared into the meeting by any authorized participant. Meetings can be recorded with the click of a single button.
- **WebEx Event Center:** Allows for large-scale meetings. Tools are provided for successful delivery of online events, including planning/promotion, event delivery, and follow-up campaign reporting.
- **WebEx Training Center:** Provides an education-focused, interactive environment. This includes video capabilities, breakout sessions for discussion, and labs. Reporting is provided on a per-attendee basis, showing participation level. (Any time WebEx is not the primary application on the screen, an indicator is placed by the attendee name and the time away from the main screen logged.)
- **WebEx Support Center:** A customer support meeting interface primarily aimed at remote desktop and content sharing for real-time IT support and customer service regardless of geographical separation.

Cisco has expanded the cloud-based capabilities of WebEx services by introducing the Collaboration Meeting Room (CMR). CMR provides the capability to use cloud-based videoconferencing infrastructure rather than a company needing to purchase its own on-premises infrastructure. CMR allows the creation of user-specific, personalized WebEx meeting rooms. These rooms can be scheduled or launched instantly. If there is already an existing on-premises Cisco TelePresence implementation, a CMR Hybrid (formerly known

as WebEx-enabled TelePresence) solution is available which will allow the bridging of on-premises video infrastructure and the Cisco WebEx cloud-based video infrastructure. This provides a seamless meeting experience for all users whether attending via WebEx or Cisco TelePresence collaboration endpoint. Shared content from either side is presented instantly to the other side.

WebEx also provides a cloud-based instant messaging solution known as Cisco WebEx Messenger (formerly known as Cisco WebEx Connect IM). It provides presence information and enterprise IM. It can be integrated with Cisco Jabber for a single client experience using on-premises or cloud-based call control and on-premises or cloud-based IM. The two components may be implemented independently of one another.

Cisco's on-premises conferencing solution is known as Cisco WebEx Meetings Server (CWMS). It allows up to 2000 ports of connectivity for on-premises meetings. CWMS is essentially a locally based instance of WebEx Meeting Center. It has most of the same capabilities but does not quite scale to the same extent as its web-based counterpart. CWMS does not support the CMR Hybrid type of solution.

Collaboration Endpoints

A more in-depth discussion of the Cisco collaboration endpoints is covered in Chapter 5, "Cisco IP Phones, Desk Endpoints, and Jabber Overview," but there is a need to cover them here, to a small degree, simply to provide clarity as to their place in the overall architecture. The endpoints available are varied and quite diverse in capability. An endpoint can be a simple desktop phone such as the Cisco 3905; a highly functional, feature-rich endpoint such as the Cisco DX650; or anywhere in between. The primary focus in deciding which endpoint goes where depends on the use of said endpoint and the requirements of the persons using the endpoint.

The portfolio of available Cisco collaboration endpoints is quite diverse. The features range from simple dial tone to a full immersive Cisco TelePresence room-based unit such as the Cisco IX5000. As the capability and available feature set of each endpoint increases, so will its price, in general. A number of exceptions apply on that front where there are transitions in progress between the older models and the newer ones. Regardless, from the perspective of the CUCM administrator, every endpoint is treated the same. All are treated as phones within the pages of the administration web application.

Within the portfolio are software-based endpoints, physical desk phones, personal video endpoints, and room-based immersive video endpoints. The endpoints specific to the discussion surrounding the exam include the following:

- Cisco 8900 Series phones – 8945 and 8961
- Cisco 9900 series phones – 9951 and 9971
- Cisco TelePresence EX series endpoints – EX60 and EX90
- Cisco DX series endpoints – DX650
- Cisco Jabber software clients – desktop, smartphone, and tablet

- Cisco TelePresence SX Quickset series endpoints
- Cisco TelePresence Integrator C series endpoints
- Cisco TelePresence room endpoints – CTS1100, MX200, MX300, and Profile series
- Cisco TelePresence immersive endpoints – TX1310 and TX9000 series

There are obviously significant changes to the portfolio as new endpoints are being released constantly. At the time of this writing, the DX70 and DX80 have been added to the portfolio along with numerous updates to the room and immersive series of endpoints, including the MX700, MX800, IX5000, and more. For purposes of this book, the focus is on the coverage dictated by the exam blueprint.

Cisco Collaboration Architecture

The Cisco collaboration solution is broken into service domains. The concept of a service domain is discussed at various points throughout the book. It is somewhat, though not entirely, synonymous with the technology categories listed at the beginning of the "Introducing Cisco Collaboration Solutions" section earlier in this chapter. The primary difference is that the service domain takes a more specialized view. Figure 4-5 shows an overview of the Cisco collaboration service domains.

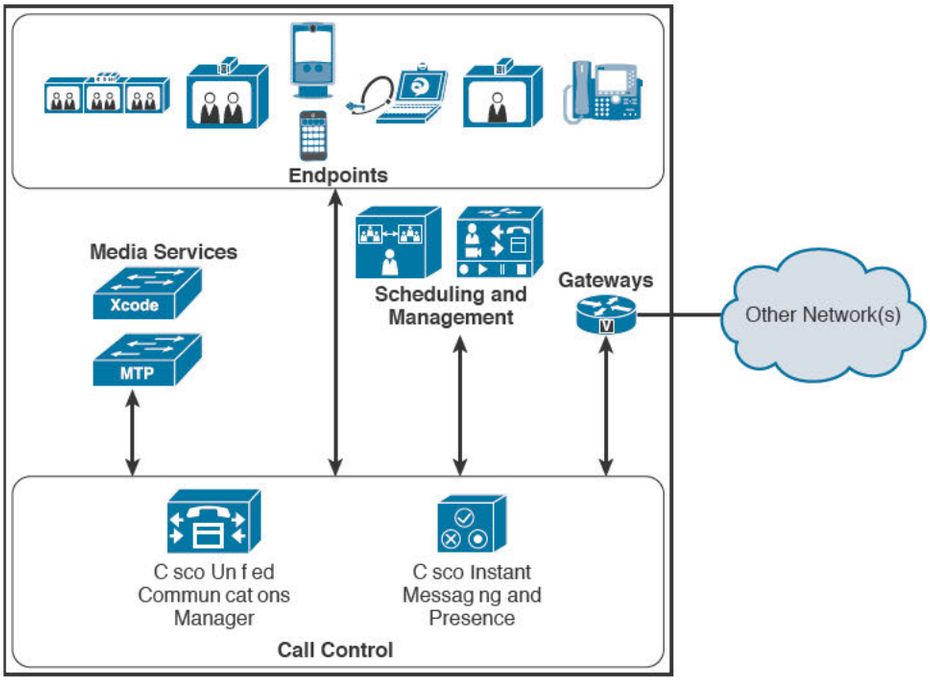


Figure 4-5 *Overview of the Cisco Collaboration Service Domains*

Whereas unified communications encompasses multiple aspects of the collaboration solution, the service domain focuses on only one aspect. The service domains of particular importance in this discussion include the following:

- **Call control:** A central entity within the infrastructure that is in charge of call/session control, dial plan, and routing decisions for setup, maintenance, transfer, teardown, and other signaling aspects associated with end-to-end communications. Call agents (a.k.a. endpoints, gateways, media services) attach to, and register with, the call control plane to make use of call-based services, web-based services, and other media-based applications or services.
- **Endpoints:** The user interface to the collaboration infrastructure. This includes desk phones, video endpoints, immersive room systems, desktop clients, smartphone clients, tablet clients, and other advanced collaboration user systems.
- **Gateways:** Connectivity to other systems and their associated network infrastructure. This includes analog systems, PSTN connectivity, legacy PBX connectivity, SIP trunking connectivity, business-to-business (B2B) connectivity, vendor-proprietary systems, and more.
- **Media services:** Audio and video media services, whether point-to-point (P2P) or multipoint (P2MP). This includes conference bridging resources (audio/video), music-on-hold services, annunciator services, media termination point (MTP) services, audio/video recording services, transcoding services, and so on.
- **Scheduling and management:** Centralized management services for collaboration endpoints, conferencing resource reservation/scheduling, videoconference layout customization, endpoint bandwidth management, and more. It is common for these systems to integrate with both e-mail services on the back end and e-mail clients at the user interface.

Call Control

Of all the service domains, call control is the most important simply due to the fact that every other aspect of the Cisco collaboration architecture relies on it as the common foundation. Even the other service domains depend entirely on the existence of the call control plane to function.

Over the course of the evolutionary path of both voice and video technologies, call control has come in numerous flavors, including both standards-compliant and non-standards-compliant (that is, proprietary) forms. The technologies have come a long way since the creation of the first phone, the first camera (still/video), the first telephone switch, and so on. Call control from Cisco's perspective now rests squarely upon Cisco Unified Communications Manager. This is the case both for on-premises solutions and hosted solutions.

With the acquisition of TANDBERG, Cisco greatly increased the pace of innovation in the video communications market. The heart of the TANDBERG infrastructure included the Video Communications Server. VCS can operate independently of CUCM, certainly. It has done so for quite a long time before Cisco's acquisition of TANDBERG. VCS is a video aggregation and call processing engine for standards-based video endpoints. It provides not only for H.323 and SIP endpoints, but also interworking between the two protocols. VCS is discussed in a bit more detail later in the "VCS and Cisco Expressway" section.

Signaling

CUCM is primarily a signaling entity. It handles call routing, call setup, call teardown, transfers, media resource allocation, and much more. With exceedingly few exceptions (for example, CUCM node-based software conference bridging), CUCM does not actually handle the media generated by the calls that it manages. There are two general flavors of signaling: line-side and trunk-side signaling. They are exactly what their names imply. There is a wide array of potential protocol options for both sides, and they tend to be somewhat independent of one another. Line-side signaling refers to the operations performed between CUCM and registered telephony devices such as IP Phones, analog terminal adapters (ATAs), analog voice gateways, and the like. Trunk-side signaling deals with operations performed between CUCM and other voice/video call control elements, such as PBXs, provider PSTN infrastructure (whether through SIP or TDM-based connections), other CUCM clusters, and so on.

Since CUCM came about in the late 1990s, it has primarily made use of a proprietary line-side protocol known as the Skinny Call Control Protocol (SCCP). The Skinny protocol was used due to the fact that CUCM, then known as Cisco CallManager, was able to provide a feature set that was out of reach of the existing standards of the day: H.323 and Session Initiation Protocol (SIP). SIP line-side protocol simply was not evolving at a pace rapid enough to meet the demands of businesses for enterprise-grade telephony. The traditional PBX vendors, still using proprietary analog and digital telephony suites, have been providing a significant array of feature options in their solutions for decades. Skinny enabled Cisco to offer a very large percentage of the most commonly used, and therefore demanded, features. This is what allowed Cisco to gain a foothold in the telephony market and pull immense market share away from the traditional PBX vendors.

In recent years, SIP has made great strides. Finally, SIP has reached feature parity with Skinny. As with the bulk of Cisco's proprietary offerings, once the industry standard catches up, they make the switch. Nearly all the endpoints produced today are primarily SIP devices. Many endpoints can use either one depending on the desire of the customer. However, SIP is becoming more and more the sole focus, and Skinny is moving into retirement. That is not to say, however, that it will not be supported. It certainly will be. It just will not be the first choice or primary focus for new features and functionality.

Cisco's move to SIP is not solely relegated to IP Phones. Cisco video endpoints also are predominantly SIP based as well. From the standpoint of CUCM, endpoints are endpoints. It does not matter whether they are IP Phones, video endpoints, or immersive TelePresence room systems. To CUCM, they are simply endpoints. There is fundamentally no difference in the way they are administered. CUCM does use a standards-compliant SIP implementation. This means that a CUCM-registered SIP endpoint can communicate with nearly any other standards-compliant SIP endpoint in existence.

CAC

Another feature provided by CUCM is call admission control. CAC is a mechanism that allows CUCM some visibility into network infrastructure to enable it to protect the user experience by making sure that sessions (voice/video) that are in progress cannot be

negatively impacted by the setup of additional sessions following the same path. Two mechanisms in use currently accomplish this:

- **Topology-unaware CAC:** Accomplished by manually configuring static location information in CUCM and specifying bandwidth capabilities between each individual location and the other configured locations. CUCM tracks calls between the locations and will not allow the stated session bandwidth to be exceeded.
- **Topology-aware CAC:** Accomplished based on the ability of the CUCM to communicate with the network about available resources. This enables it to dynamically adjust call admission parameters based on topology changes, such as outages or other convergence events. Topology-aware CAC relies on real-time protocols to report back on availability of network resources across all paths throughout the network.

Without CAC, in one form or the other (though the preference is definitely topology aware), an unlimited number of sessions could be set up between locations. At some point, bandwidth will become overused, and the traffic flow of all sessions will suffer. If only a certain amount of bandwidth is seen by CUCM as being available between two locations, it will not allow a session to be set up in excess of the threshold, thereby protecting all the existing calls in progress.

Unified Dial Plan

Another overwhelming benefit provided by CUCM is a unified dial plan. As the voice and video worlds evolved, each maintained its own mechanisms for dialing remote endpoints. In the voice world, phone numbers, extensions, and directory numbers (DNs) ruled. In the video world, there has been a great deal of reliance on dialing by IP address and dialing based on a more simplified scheme such as that used by SIP, the uniform resource identifier (URI). A URI is merely a more user-friendly format using *username@domain.tld*, very much like an e-mail address. H.323 was able to make use of a similarly simplified format.

CUCM supports the use of phone numbers in the traditional voice sense, but it also supports the use of URI formatted dialing. This allows for the removal of numeric dialing entirely, should such be desired. Simply by knowing the e-mail address (which, you can consider URIs to be here, for the sake of simplicity) of someone with whom you want to communicate, you may do so. For all intents and purposes, the URI provides a very user-friendly means of reaching someone on any device, be it a phone, mobile device, video endpoint, immersive room, or other, without the need to remember or even store phone numbers for each different device. CUCM takes care of the URI/phone number association.

VCS and Cisco Expressway

Cisco VCS is not only a call control and registration mechanism for video endpoints; it also provides firewall-traversal services so that video endpoints outside the network can securely connect to endpoints inside the network while maintaining the viability of the firewall itself by removing the requirements for opening large port ranges to the outside world. This is accomplished by the use of two VCS devices. One of these is inside the firewall and known as VCS Control (VCS-C). The other is placed outside the firewall, or more preferably in a demilitarized zone (DMZ), and is known as VCS Expressway (VCS-E).

VCS-C handles all internal endpoints and calls. VCS-E handles calls inbound from outside the network, allowing them to make contact with endpoints and MCU resources on the inside of the network. That said, two essential types of calls are handled:

- **Traversal calls:** Any call requiring VCS to pass call media and signaling. This might be a call from the inside of the network to the outside or vice versa. This also includes any interworking calls (H.323 <-> SIP or IPv4 <-> IPv6), calls wherein the endpoints are on opposite sides of a Network Address Translation (NAT) implementation, any calls passing inbound on one LAN port and outbound on another for the same VCS (dual network interface card [NIC]), and all encrypted calls.
- **Nontraversal calls:** Any call that is not a traversal call. That is, the VCS processes only signaling traffic.

Figure 4-6 illustrates the VCS architecture and the concepts of traversal and nontraversal calls.

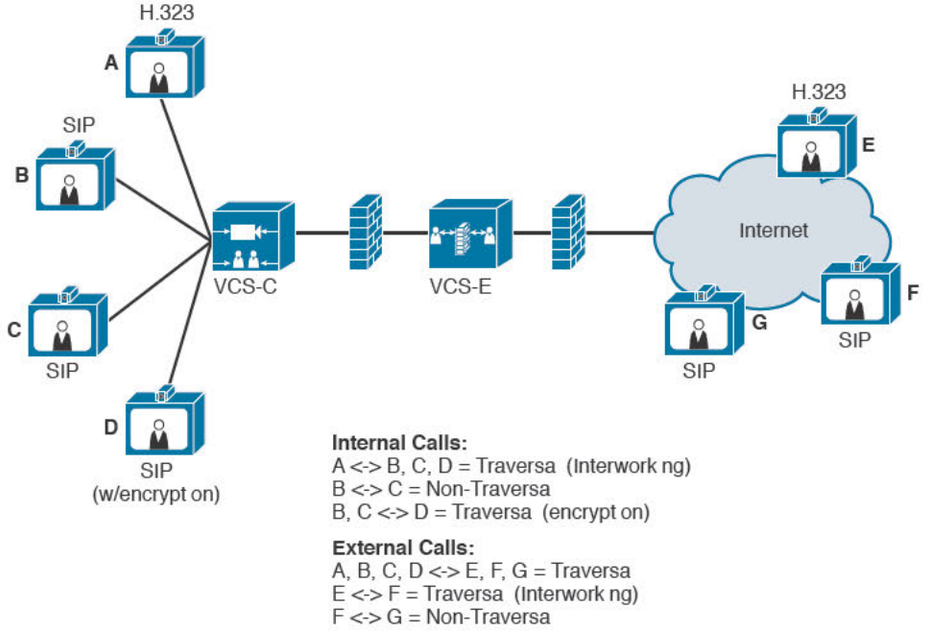


Figure 4-6 *Cisco VCS Architecture*

Cisco has continued building on that architecture to add additional features, innovations, capabilities, and more. The existence of multiple call control elements in a single environment, in this case CUCM and VCS, has long been a source of added complexity. Keeping the two in harmonic balance tends to be an interesting exercise in terms of ensuring proper call routing, endpoint registration, and so on. Initially, the integration capabilities between CUCM and VCS were somewhat limited. The creation of a SIP trunk between the two entities for call routing was essentially all that could be done. Each maintained its own autonomy from a dial plan perspective. Calls inbound or outbound were passed between

the two, often with significant manipulation of the called-party number being necessary to facilitate the call setup. This is because, traditionally, CUCM did not support URI dialing natively, where VCS has done so since its creation. The domain portion of the URI had to be stripped or added as appropriate for the call direction. URI dialing support has since been added to CUCM with version 9.x and later.

Cisco has released a new twist on the VCS firewall-traversal mechanism that allows for multiple traffic types to make use of the secure connection. This new architecture is known as *Cisco Expressway*. Under the hood, Expressway is still VCS, albeit a slightly scaled-down version of VCS in terms of total functionality. A number of the former VCS functions are now handled by CUCM. For example, it does not need to actually register endpoints as it has in the past. All endpoints register to CUCM. So, it is VCS made somewhat subservient to CUCM. Expressway supports video, voice, content sharing, voice mail, presence, and IM traffic over the same connections rather than simply video traffic. This feature set is known as Mobile and Remote Access (MRA). This brings to light the two additional manners in which VCS can be deployed: Expressway-C and Expressway-E. The Expressway-C and Expressway-E variations have the same essential function and deployment locations within the architecture as their VCS-C and VCS-E counterparts. Expressway-C is deployed inside the firewall, whereas Expressway-E is deployed in the DMZ or outside the firewall. External calls, business-to-business (B2B) calls, and interoperability/interworking calls still have the same requirements in terms of traversal/nontraversal calls, although they are now known as Rich Media Sessions (RMSs).

Expressway architecture provides a means of allowing VPN-less access to collaboration resources to clients and endpoints outside the network. Gone are the days wherein a virtual private network (VPN) tunnel was required on each device that wanted to access corporate collaboration services. Expressway provides secure firewall traversal and line-side support for CUCM registrations. Expressway is also the mechanism that allows the use of the CMR Hybrid capability. Figure 4-7 shows how the Expressway architecture ties into the Cisco Preferred Architecture for collaboration.

Note that not all endpoints are supported with the MRA functionality. At present, the 7800 series, 8800 series, and EX and DX series endpoints are supported for external connectivity. In addition, the newer lines of SX, MX, and IX series TelePresence endpoints are supported.

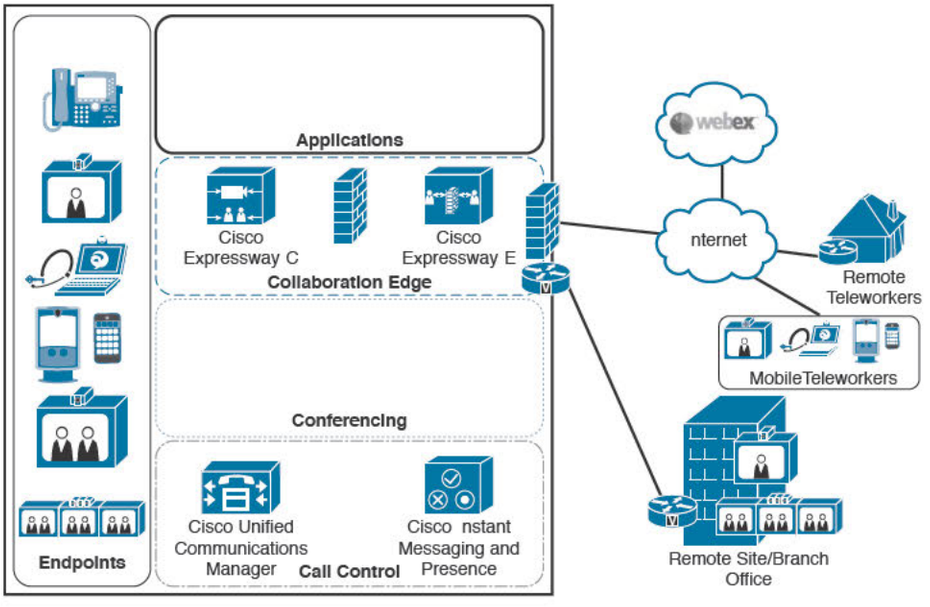


Figure 4-7 *Cisco Expressway Architecture*

Endpoints

As has been discussed already in this chapter and others throughout the book, endpoints make or break the solution. They are the user interface to the collaboration system. If the endpoints are difficult to use, provide a poor user experience, or are simply inelegant, the user community will cease to use them and find alternative means of communication. These are often fragmented, suboptimal solutions. The result is employee and customer dissatisfaction resulting in reduced productivity and loss of revenue.

The focus for Cisco collaboration endpoints is aimed at a delightful user experience and ease of use. The 7800, 8800, and DX series phones are all a result of this focus. The same is true for the newer lines of Cisco TelePresence endpoints: the SX, DX, and IX series units.

Obviously, there are significantly more Cisco endpoints deployed other than these. Cisco understands and wholeheartedly supports the concept of investment protection. With that in mind, the capabilities of existing endpoints and codecs have been immensely enhanced as well. In many customer environments, CUCM has not yet been implemented or has been implemented only for IP Phones. In those environments, VCS remains the registration point and call control element for video endpoints, codecs, MCU resources, and so on. This

brings up the discussion point of there being two flavors, or variants, of Cisco TelePresence endpoints, as follows:

- **Cisco TelePresence software-based endpoints:** These include the Cisco CTS endpoints such as the CTS500, CTS3000, TX1310, and TX9000 series units, which are typically SIP based and register directly to CUCM for call control and management via HTTP. The CTS line of TelePresence endpoints has reached end of sale/life, although they are still supported.
- **Cisco TelePresence TC software-based endoints:** These include the former TANDBERG endpoints and codecs such as the EX series endpoints (EX60, EX90), the C series codecs (C20, C40, C60, C90), and the Cisco TelePresence MX and SX series codecs. These are all capable of registering to VCS (H.323 or SIP) or CUCM (SIP).

Endpoints deployed in H.323 deployments would use the TC software, register to VCS, and then would be managed/configured via Cisco TelePresence Management Server (TMS). In fact, TMS is capable of managing not only Cisco H.323 and SIP endpoints, but also third-party standards-compliant endpoints as well. Even now, with VCS taking on the role of the Expressway function within the Cisco Collaboration Architecture, TMS is in widespread use and is still a requirement for management and scheduling of video resources (though its role has changed slightly in that it works with CUCM and Cisco TelePresence Conductor to manage videoconferencing resources).

Gateways

Gateways perform a vital function within the Cisco collaboration architecture. They are the interface to external or disparate network infrastructures. While the word *gateway* seems a rather generic term, in this discussion it is understood to mean a voice/video gateway specifically.

Voice gateways take the form of traditional Cisco routers such as the Cisco Integrated Services Router (ISR) series routers or mission-specific gateways for high-volume analog connectivity such as the VG224 or VG350. There also are lower-volume analog gateways such as the VG202 and VG204. The type of gateway deployed depends on the required connectivity and type of endpoints to be serviced. A voice gateway, such as a 2900/3900 ISR, can contain multiple interface types ranging from analog foreign exchange station (FXS), foreign exchange office (FXO), or ear and mouth (E&M) ports to digital T1 CAS or PRI ports. These can be used in any combination required and allowed by the real estate provided within the router chassis. A gateway can also be focused entirely on IP-based connectivity for H.323 call routing or SIP trunking.

From a video perspective, the gateway functionality is somewhat similar. It connects disparate networks and provides a bridge between the transport mechanisms on the ingress and egress ports. In the legacy video architecture, there was some discussion of an ISDN gateway. This gateway is similar to what would be deployed in the traditional voice gateway infrastructure. PRI circuits are an ISDN technology. It is merely their purpose that changes based on the traffic transported. There has been significant usage of ISDN BRI in the data world, but it has rapidly waned and is all but nonexistent today. From a video perspective, it seems to be hanging on, gasping for life. To that end, the ISDN gateway is still a viable, and somewhat commonly encountered, entity in video deployments.

Gateways are also used to transcode between dissimilar technologies. Transcoding gateways actually terminate the inbound RTP media stream in one format and re-originate the stream in the other format. The Cisco Advanced Media Gateway (AMG) was created specifically to provide a mechanism to transcode Microsoft's proprietary RTAudio/RTVideo media formats to standards-based H.263 format to allow it to be viewed on non-Microsoft Lync/OCS endpoints. Without the transcoding capabilities, the only common format supported between Microsoft Lync/OCS and standards-compliant video endpoints is Common Intermediate Format (CIF) video. CIF is a very low-quality format and usually deemed inadequate for enterprise communications.

With the release of Lync 2013, the AMG is no longer necessary, as Microsoft has deprecated the use of RTAudio/RTVideo in favor or their own variant of H.264. When Microsoft announced that they were moving away from RTAudio/RTVideo, dropping support of H.263, and implementing H.264, there was great hope that they would move away from their traditional closed, proprietary nature entirely; however, the hope was short-lived. Although the media is indeed H.264 video, the signaling in Lync 2013 remains proprietary. So, at once, the AMG became obsolete, and the need for a new means to transcode between Lync 2013 and standards-compliant video arose.

As more and more customers tire of the compatibility games and simply demand interoperability, Cisco implemented a native interoperability function within the Expressway architecture. This allows Microsoft Lync and standards-compliant video endpoints to communicate natively via the use of a Rich Media Session (RMS) license.

In the Expressway architecture, all licensed users for CUCM endpoints are also entitled to make use of the RMA functionality at no additional cost. That is, they can make use of any RMA-supported device inside or outside the network without additional licensing. Recall that any call making use of the firewall-traversal mechanism would use a traversal license. Traversal licenses were not free by any means. Under Cisco's licensing with CUCM 9.x and later, the ability to make use of the traversal mechanism is built in to every User Connect License (UCL) Enhanced (1 device per user), UCL Enhanced Plus (2 devices per user), and Cisco Unified Workspace License (CUWL) (10 devices per user).

Just as B2B and interoperability calls required traversal licenses in the past, they require RMS licenses now. So, the rules defining traversal and nontraversal calls still apply.

Media Services

Media services is a high-level descriptor for management and allocation of media resources. Media resources, in terms of the collaboration architecture, deal primarily with audio conferencing or videoconferencing resources. However, it does include additional components such as music-on-hold, MTP, transcoding, and more. From the exam perspective, the focus of media services will fall squarely on conferencing.

In general terms, there are ad hoc conferences, meet-me conferences, and schedule conferences. This is true for both audio conferences and videoconferences.

A conference, regardless of type, includes three or more participants and requires some kind of bridging resource (that is, a resource that mixes all the media from all sources and transmits the combined media stream to all participants).

For audio conferencing, CUCM has some default software conference bridging capabilities built in. If greater scale is needed, a hardware conference bridge resource consisting of digital signal processors (DSPs) is required. A Cisco ISR conference bridge will contain some number of Packet Voice Digital Module (PVDM) resources. The current generation of ISRs (2900/3900/4400 series routers) is using PVDM3 modules. PVDM3 modules contain between 8 and 256 DSP channels. These resources are registered to CUCM as a conference bridge resource and those resources invoked when required. PVDM3 modules can also handle some degree of videoconferencing, but they are not necessarily optimized to do so. Note that although the older PVDM2 hardware can be used in these ISRs (via installation in a network module such as the NM-HDV), the coexistence of PVDM2 and PVDM3 resources in a single chassis is not supported. If both are detected, the PVDM2s will be shut down.

Cisco TelePresence MCUs are hardware resources specifically created to deal with videoconference bridging. MCUs come in many shapes and sizes depending on the number of conferences, number of attendees per conference, resolution desired, and desired video codec support. The hardware can support multipoint collaboration up for full high-definition (HD) video at 720p60 or 1080p60. This includes high-density support for various conference views, including continuous presence and picture-in-picture (PIP). These hardware resources also support multiple formats and adaptive rate matching to provide the best possible experience to a wide array of standards-compliant endpoints, be they H.323 or SIP.

The hardware MCU is giving way to virtualized resources in the form of the Cisco TelePresence Server (CTS). The CTS can be hardware based or software based. The hardware-based version is essentially a virtual server running on a blade in an MCU chassis. CTS supports conferencing services for both H.323 and SIP endpoints as long as they are standards compliant. The software version can run on a VMware ESXi host on nearly any supported hardware platform.

The Cisco Virtual TelePresence Server (VTS) is a virtualized appliance for extremely high-density videoconferencing. This includes enhanced view modes, multiscreen, active presence, multivendor interoperability, and multistream. Multistream is a new Cisco feature that allows the use of multiple screens both for videoconference and content sharing.

Another aspect of media services for Cisco videoconferencing is the Cisco TelePresence Content Server (TCS). TCS is a software-based virtual appliance that provides recording, live streaming, and on-demand sharing of videoconference content. The content can then be distributed to any PC or portable media device, or it can be posted to a Cisco Show and Share portal. The recording function can be invoked manually, scheduled as a videoconference resource to automatically record the call and all shared content, or it can be invoked for every call. To invoke the TCS manually, the URI of the TCS is simply conferenced into the call.

Cisco TCS supports the use of Cisco video endpoints or any standards-compliant H.323 and SIP video endpoints. It can connect easily to Cisco MCU resources and is tightly integrated with Cisco's scheduling and management platform.

Note When interworking between H.323 and SIP endpoints is required, including the use of the MCU, CTS, VTS, TCS, and so on, either Cisco VCS or Cisco Expressway is necessary to provide that functionality. When VCS is in play, a traversal license is used for each H.323 endpoint. For Expressway, an RMS is used.

Scheduling and Management

The scheduling and management of Cisco video endpoints and conference resources is performed primarily by the Cisco TelePresence Management Server (TMS). TMS is a Microsoft Windows Server-based software package geared specifically for providing a web browser-based interface (using Microsoft Internet Information Services and the .NET Framework) to the video units, available resources, and more. The Microsoft Windows Server installation can be virtualized or installed on a bare-metal server. Obviously, Cisco prefers the use of Cisco UCS platforms, but the only real requirement is that the Microsoft Windows Server and its hardware platform meet the required specifications.

TMS offers the capability to control and manage multiparty conferences, infrastructure, any standards-compliant endpoints, and more. This includes feature augmentations such as one-button joining of a meeting. Shortly before the scheduled start time of the meeting, a button shows up on the video endpoints scheduled to join a particular conference. At meeting time, a participant merely touches the button to join or initiate the conference. TMS integration with Microsoft Exchange and Outlook combine to provide a flexible, easy interface for quick conference scheduling and resource booking options. On the back end, TMS can integrate with Microsoft Exchange for scheduling through Microsoft Outlook clients. From a user perspective, an installed plug-in allows the use of an intuitive scheduling tool right from an end user's Microsoft Outlook client. The one-button-to-push meeting access feature is available in TMS 13.1 and later.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 4-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 4-2 Key Topics for Chapter 4

Key Topic Element	Description	Page Number
List	Describes the three basic types of conferences	53
Section	Describes various circuit types in use with legacy video architecture	56
Section	Discusses the basic evolution of call control capabilities for video endpoints	59
Paragraph	Defines unified communications and the various capabilities that are most typically associated with the term	62
Section	Specifies the Cisco collaboration endpoints most relevant to the exam	64
Paragraph	Describes connection admission control in process and purpose	67
Paragraph	Describes the solutions provided by both Cisco VCS and Cisco Expressway and how they differ in general use and purpose	68
Paragraph	Explains various types of available gateways in use with Cisco Unified Communications solutions	72
Paragraph	Explains the concept of media services and what it means to the success or failure of a collaboration architecture	73

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

2B+D, 23B+D, 30B+D, analog terminal adapter (ATA), Basic Rate Interface (BRI), call admission control (CAC), call control, Common Intermediate Format (CIF), Cisco Unified Communications Manager (CUCM), Collaboration Meeting Room (CMR), CMR Hybrid, Cisco TelePresence Server (CTS), Cisco WebEx Meetings Server (CWMS), digital signal processor (DSP), E1 CAS, E1 PRI, Expressway-C, Expressway-E, firewall traversal, gatekeeper, gateway, H.263, H.264, H.320, H.323, Integrated Switch Digital Network (ISDN), multipoint control unit (MCU), Mobile and Remote Access (MRA), nontraversal call, private branch exchange (PBX), Packet Voice Digital Module (PVDM), quality of service (QoS), Rich Media Session (RMS), Skinny Client Control Protocol (SCCP), Session Initiation Protocol (SIP), T1 CAS, T1 PRI, TelePresence Content Server (TCS), TelePresence Management System (TMS), traversal call, Unified Contact Center Enterprise (UCCE), Unified Contact Center Express (UCCX), universal resource identifier (URI), Video Communications Server (VCS) Control, Video Communications Server (VCS) Expressway, Virtual TelePresence Server (VTS), WebEx Event Center, WebEx Meeting Center, WebEx Meetings Server, WebEx Support Center, WebEx Training Center

This chapter covers the following topics:

- **Cisco IP Phone Portfolio:** This section provides an overview of the features and capabilities of the currently available Cisco IP Phone models.
- **Cisco Collaboration Desktop Endpoints:** This section briefly discusses the Cisco EX series and DX650 desktop collaboration endpoints.
- **Cisco Jabber Software Clients:** This section provides a high-level description of the Cisco Jabber software client and platforms on which it is available.

Cisco IP Phones, Desk Endpoints, and Jabber Overview

To simply state that the Cisco endpoint portfolio is extensive and diverse is an immense understatement. The portfolio has evolved greatly since the first Cisco IP Phones were made available after the Cisco acquisition of Selsius in 1998. At that time, the true advance in technology was the fact that the phone was an Ethernet-connected device running a TCP/IP stack and capable of providing basic telephony features. A possibly-not-so-well known reference to Selsius remains in the system to this day. When adding endpoints to the Cisco Unified Communications Manager (CUCM), devices are shown with a device name similar to this: SEP000CABCDEF12. The hexadecimal portion is the Media Access Control (MAC) address of the device being added. The SEP stands for Selsius Ethernet Phone.

Cisco has slowly started to move away from differentiating IP Phones, software-based clients, desktop video endpoints, and immersive TelePresence room-based video endpoints. In the past, the distinction was important. Now the lines are blurring. These endpoints all have similar characteristics at the most basic levels and can be managed in a nearly identical manner.

It seems that video has become an increasingly vital means of communication. This means that video capabilities must move from that one conference room or the executive board rooms into the masses.

Every device must allow people to communicate in the manner of their own choosing. So, IP Phones, whether video capable or not, are simply collaboration endpoints. Whether the device in question is an IP Phone, software client, desktop video endpoint, or an immersive video endpoint in a conference room, it is simply a collaboration endpoint. Making a video call is now easier than making a traditional voice-only call.

This chapter focuses on the Cisco IP Phone portfolio, collaboration desk endpoints, and the Cisco Jabber soft client (in its various forms). But, remember: They are all simply endpoints.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the “Exam Preparation Tasks” section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 5-1 lists the major headings in this chapter and their corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes.”

Table 5-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco IP Phone Portfolio	1–5
Cisco Collaboration Desktop Endpoints	6–8
Cisco Jabber Software Clients	9–10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which Cisco IP Phone is Gigabit Ethernet capable?

   a. 3905
   b. 7821
   c. 7841
   d. 7861

2. What is the maximum number of lines supported by the Cisco 7965 IP Phone?

   a. 1
   b. 2
   c. 4
   d. 6

3. With which of the following handsets can the 7916 expansion module be used?

   a. 7945
   b. 7942
   c. 7965
   d. 7861

4. Which phone is built to function in hazardous environments, such as those in which there is a risk for atmospheric explosible gases?

   a. 7926G
   b. 7925G
   c. 7925G-EX
   d. 7921

5. Which phone supports VGA quality video, Bluetooth, and Wi-Fi?

   a. 9971
   b. 9951
   c. 8961
   d. 8945

6. The DX650 operating system is based on which of the following?

   a. Android (Jellybean)
   b. Blackberry
   c. Apple iOS
   d. Windows Mobile

7. The Cisco DX650 is supported beginning with which version of Cisco Unified Communication Manager?

   a. 4.1.2
   b. 10.5.2
   c. 8.0.3
   d. 7.1.5

8. Which of the following supports the multisite feature?

   a. EX60
   b. EX90
   c. DX650
   d. 8831

9. Which of the following does Cisco Jabber for Windows use for desk phone control?

   a. CTI
   b. SIP
   c. SCCP
   d. JTAPI

10. What protocol does Jabber use for instant messaging functionality?

    a. SIP
    b. SCCP
    c. XMPP
    d. CDP

Foundation Topics

Cisco IP Phone Portfolio

The Cisco IP Phone portfolio consists of a rather wide array of options and feature sets. This diversity of features allows flexibility in deployment based on the needs of the individuals using the phone and the phone's general purpose (lobby phone, break room phone, conference room phone, and so on). There is no one-size-fits-all mindset when it comes to collaboration technologies. Different users will have different needs/desires in how and where they choose to communicate. The focus rests squarely on creating the best user experience regardless of the devices in question.

This section covers the following Cisco IP Phone models:

- 3900 series
- 7800 series
- 7900 series
- 8800 series
- 8900 series
- 9900 series

The order of discussion is merely based on numeric value of the series rather than form, functions, or features. The most up-to-date information about all Cisco collaboration endpoints is available here:

http://www.cisco.com/c/en/us/products/collaboration-endpoints/index.html

Cisco 3900 Series Phones

The 3900 series currently contains only the 3905 model as of the time of this writing. Its predecessors, the 3911 and 3951, were retired in 2010. So, there is no real need to cover them here.

The 3905 is an entry-level, single-line, SIP-only handset. It addresses the need for basic dial tone at a very cost-effective price point. It is a single-line device, although it does support call-waiting. It has a small 128x32 pixel monochrome display but no programmable soft keys. Therefore, it does not support XML applications. It is Class 1 Power over Ethernet (PoE) capable or can use an external power supply. It has an integrated 10/100 switch and speakerphone as well. Figure 5-1 shows the 3905 model phone.

Figure 5-1 *Cisco 3905 IP Phone*

As seen in the figure, there is a Message Waiting Indicator (MWI) in the top-right corner. It has eight fixed feature keys that provide access to several functions. The buttons just below the display include a Previous button (to go back one menu level), up and down navigation buttons, along with a Select button and a Settings button for phone configuration.

Just below the navigation pad is a row of three feature keys. These keys, from left to right, are Redial, Transfer, and Hold/Resume. Below the keypad is an additional row of buttons for Mute, Volume Control, and Speakerphone. Table 5-2 provides a feature overview of the 3905 IP Phone.

Table 5-2 Cisco 3905 IP Phone Features

Feature/Function	Characteristics
Integrated switch	10/100
Display	128x32 monochrome LCD
Speakerphone	Yes
Line keys	1
Programmable soft keys	0
Fixed feature keys	8
MWI	Yes
XML support	No
Headset port	No
Signaling protocol	SIP
PoE class	Class 1

As is evident, the 3905 is purpose built to provide phone service in a hospital waiting room, hotel lobby, college dorm room, break room, hallways, or anywhere else requiring a simplified feature set. The phone can be wall-mounted or simply placed on a desk or tabletop.

Cisco 7800 Series Phones

Key Topic

The Cisco 7800 series phones are relatively new on the scene. They include a number of interesting enhancements over many of their IP Phone predecessors. These phones are designed for light- to high-use voice users and are meant to replace the recently retired 6900 series phones.

As IP Phone deployments grow and place very increasing demands on edge switch PoE capabilities, it becomes clear that there is a need for a high-feature phone with low power requirements. As Class 1 power devices, the 7800 series phones are built for just such environments.

There are three models in the 7800 series line:

- 7821
- 7841
- 7861

Each includes wideband (G.722) audio support and backlit grayscale displays and supports only SIP signaling. In addition, these phones support the Electronic Hookswitch feature used in many industry headsets today. They can be wall-mounted or placed on the desktop. Each model is available in charcoal or white.

Note The 7841 is the only model in the series that includes Gigabit Ethernet capabilities.

Figure 5-2 shows the 7800 series phones. Table 5-3 provides a feature overview.

Figure 5-2 *Cisco 7821, 7841, and 7861 IP Phones*

Table 5-3 Cisco 7800 Series Phone Features

Feature/Function	7821	7841	7861
Integrated switch	10/100	10/100/1000	10/100
Display	396x162-pixel backlit monochrome	396x162-pixel backlit monochrome	396x162-pixel backlit monochrome

Feature/Function	7821	7841	7861
Speakerphone	Yes	Yes	Yes
Line keys	2	4	16
Programmable soft keys	4	4	4
Fixed feature keys	11	11	11
Advanced features	Multicall per line Wideband audio EHS support (AUX port)	Multicall per line Wideband audio EHS support (AUX port) Gigabit Ethernet	Multicall per line Wideband audio EHS support (AUX port)
Hands-free	Yes	Yes	Yes
MWI	Yes	Yes	Yes
XML support	Yes	Yes	Yes
Signaling protocol	SIP	SIP	SIP
802.3af	Yes	Yes	Yes
PoE class	Class 1	Class 1	Class 1
CUCM version	8.5.1 and later	8.5.1 and later	8.5.1 and later

Cisco 7900 Series Phones

The 7900 series phones have long been the so-called workhorse of the line for many years now. These phones have undergone an unimaginable number of evolutions and revolutions over the years. Currently, this series includes the following models:

- 7925G
- 7925G-EX
- 7926G
- 7942G
- 7962G
- 7945G
- 7965G
- 7975G

The 7900 series phones are grouped into families of sorts. These are based on their intended use/features. That said, the models listed here are discussed in their constituent family groups.

7925G/7925G-EX/7926 IP Phones

The 7925G, 7925G-EX, and 7926 models are 802.11a/b/g wireless handsets. They are hermetically sealed to avoid contamination by dust, liquids, and so on The exterior is coated in a rubber casing to aid in handling and provide some drop protection. These handsets meet U.S. military 810F standards. Each of the models supports Bluetooth 2.0 with Enhanced Data Rate (EDR) hands-free profile. Also built in is a button for push-to-talk functionality that can be enabled via XML application integration.

One of the more interesting additions to these handsets is the introduction of an on-board Java virtual machine, which allows the handset to run Java MIDlets locally. This allows for customized content/information to be presented to the 2-inch color screen.

So, why choose one model over the others? Up to this point, they each seem relatively similar in form and function. The differences are somewhat based on the intended use of the phone and the environment in which it will be used. Figure 5-3 shows the 7925G model.

Figure 5-3 *Cisco 7925G Wireless IP Phone*

The 7925G is the general-purpose handset model and is the most widely deployed of the three. The 7925G-EX is ruggedized and built for hazardous environments. Its bright yellow color makes it stand out in any environment. It is Atmospheres Explosibles (ATEX) Zone 2 certified for use around hazardous gases, chemicals, and other potentially explosive environments. Figure 5-4 shows the 7925G-EX handset sitting in an optional speakerphone/charger cradle (compatible with all three models).

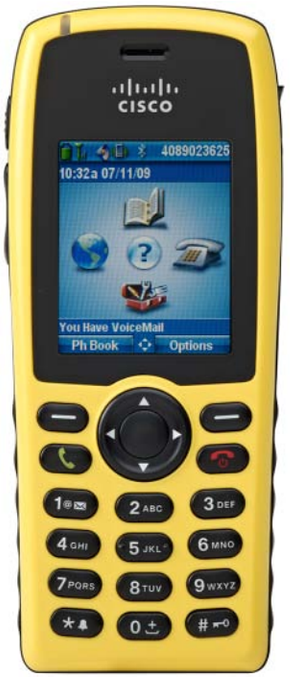


Figure 5-4 *Cisco 7925G-EX Wireless IP Phone*

The 7926G has a built-in 2D image barcode scanner. This is useful in any environment wherein inventory/assets need to be tracked. The 2D barcode scanner is not a laser-based scanner. It uses light emitting diodes (LEDs) to illuminate the target barcode and takes a picture of it, which is decoded by the phone. The resulting information is then relayed to a customer/partner developed backend system application for processing/storage. The 7926G looks identical to the 7925G in almost every way. As mentioned, the only real difference is the barcode scanner situated in the top of the handset. Figure 5-6 shows a top-down view of the handset to detail the barcode scanner.

Figure 5-5 *Cisco 7926G Wireless IP Phone Barcode Scanner*

Table 5-4 shows an overview of the features of these wireless handsets.

Table 5-4 Cisco 7900 Wireless IP Phone Features

Feature/Function	7925G	7925G-EX	7926G
Display	2-inch 176x220-pixel color	2-inch digital, 16-bit graphical TFT color	2-inch digital, 16-bit graphical TFT color
Speakerphone	Yes	Yes	Yes
Line keys	N/A	N/A	N/A
Programmable soft keys	2	2	2
Fixed feature keys	5	5	5
Advanced eatures	Bluetooth v2, push-to-talk via XML, Java MIDlet capabilities	Bluetooth v2, push-to-talk via XML, Java MIDlet capabilities, ATEX Zone 2 certification	Bluetooth v2, push-to-talk via XML, Java MIDlet capabilities, 2D barcode scanner
Hands-free	Yes	Yes	Yes
MWI	Yes	Yes	Yes
XML support	Yes	Yes	Yes
Signaling protocol	Skinny Client Control Protocol (SCCP)	SCCP	SCCP
802.11a/b/g	Yes	Yes	Yes
CUCM version	4.1 and later	4.1 and later	4.1 and later

For shared handset environments, a multicharger dock is also available. The multicharger dock can hold/charge six phones at a time.

7942G/7962G IP Phones

The 7942G and 7962G IP Phones may be the two most deployed phone models in the Cisco IP Phone portfolio at present. They are significant evolutionary steps over their predecessors in that they brought wideband audio and Internet low bit rate codec (iLBC) into widespread production. Each has a 4-bit grayscale display and dynamic backlit tricolor buttons (green/yellow/red for line status) for line appearances, speed dials, busy lamp field (BLF), intercom, or application use. The 7942 has two of these buttons; the 7962 has six. These phones can be used with either SCCP or SIP. Figure 5-6 shows the 7942G IP Phone.

Figure 5-6 *Cisco 7942G IP Phone*

The form factor shown in the Figure 5-6 is common across the 794x/796x models with only minor differences, which are pointed out as each model is discussed. Figure 5-7 shows the 7962G IP Phone.

Figure 5-7 *Cisco 7962G IP Phone*

The lower-right quadrant of the phone includes nine buttons:

- **Messages:** Provides easy access to voice mail
- **Settings:** Provides access to phone customization, configuration, and troubleshooting features functions
- **Directories:** Provides access to corporate and local directories and configured speed-dial entries
- **Services:** Provides access to XML and Java applications such as Extension Mobility (EM), time clock, weather, stock quotes, and countless other services
- **Help:** Provides access to online help pages as well as real-time call statistics and codec information while a call is active
- **Volume Control:** Provides volume increase/decrease functionality for both the handset and speaker
- **Headset:** Provides headset hookswitch control when a headset is attached
- **Mute:** Mutes the handset or speakerphone microphone
- **Speakerphone on/off:** Activates or deactivates the speakerphone function

One additional button is the blue up/down navigation pad located in the center of the phone. This button is used to scroll through available options within the phone menus or to scroll through and select individual calls when multiple calls are active.

The 7962G supports the use of up to two 7915 expansion modules (a.k.a. sidecars). The first expansion module can piggyback off of the PoE supplied to the phone by the access switch or external power supply.

Note The 7915 is not supported with the 7942G.

The second expansion module can be used only by adding an additional external power supply. The expansion modules easily mount to the right side of the phone, or each other, in the case of multiple expansion modules. The adjustable footstand of the phone has to be removed and replaced with a fixed footstand that supports the form factor of both the phone and the expansion modules. Figure 5-8 shows the 7915 expansion module.

Figure 5-8 *Cisco 7915 Expansion Module*

As shown in the figure, each 7915 provides 2 display page buttons (under the display) and 12 dynamic tricolor backlit buttons identical in function to the 6 buttons on the phone itself. This configuration allows each expansion module to provide a total of 24 buttons. In keeping with consistency of look and feel with the 7962G, the 7915 has a 4-bit, high-resolution, grayscale display and is not backlit. Table 5-5 shows an overview of the features of the 7942G and 7962G.

Table 5-5 Cisco 7942G and 7962G IP Phone Features

Feature/Function	7942G	7962G
Integrated switch	10/100	10/100
Display	5-inch 320x222 4-bit grayscale	5-inch 320x222 4-bit grayscale
Speakerphone	Yes	Yes
Line keys	2 (lighted)	6 (lighted)
Programmable soft keys	4 soft keys, 2 line keys (can be lines, speed dials, or programmable line keys)	4 soft keys, 6 line keys (can be lines, speed dials, or programmable line keys)
Fixed feature keys	10	10

Feature/Function	7942G	7962G
Advanced features	High-resolution screen Application integration capabilities Headset hookswitch control	High-resolution screen Application integration capabilities Headset hookswitch control Up to 2 7915 expansion modules
Hands-free	Yes	Yes
MWI	Yes	Yes
XML support	Yes	Yes
Signaling protocol	SCCP or SIP	SCCP or SIP
802.3af	Yes	Yes
PoE class	Class 2	Class 2
CUCM version	4.1 and later	4.1 and later

7945G/7965G/7975G IP Phones

The 7945G, 7965G, and 7975G add to the functionality of the 7942G and 7962G by providing 16-bit color, backlit screens, and Gigabit Ethernet capabilities. As such, these phones require additional power, bumping the power need up to Class 3 compared to the 7942G and 7962G models. To mitigate some portion of the increased power draw, these phones have a Display button placed to the right of, and in line with, the row of programmable soft keys running along the bottom of the screen. These phones can be configured with screen timeout values. When the phone is idle for an extended period of time, the screen blanks out to reduce power usage. When this happens, the display button illuminates (green). When the phone rings, or is taken off hook, the screen automatically wakes. Pressing the Display button manually wakes it. The 7945G and 7965G were developed with a similar form factor to the 7942G and 7962G. Like their cousins, these phones support either SCCP or SIP. Figure 5-9 shows the 7945G model.

It is clear from the figure that the button layout is nearly identical with the exception of the center button. The 7945G has two programmable line buttons; the 7965G has six programmable line buttons. Of course, those line buttons can be configured as lines, BLF, speed dial, intercom, or application keys. Whereas the 7942G and 7962G have an up/down navigation pad, the 7945G and 7965G have a four-way navigation pad with a Select button (signified by a check mark) in its center. Figure 5-10 shows the 7965G model.

Figure 5-9 *Cisco 7945G IP Phone*

Figure 5-10 *Cisco 7965G IP Phone*

The 7975G IP Phone adds an additional dimension of functionality with touchscreen capabilities. The touchscreen display is larger than the displays on the 7945G and 7965G. In addition, the 7975G phone has eight programmable line buttons and five programmable soft key buttons. Due to those factors, the form factor on the 7975G is slightly larger than the 7945G and 7965G. Figure 5-11 shows the 7975G phone.

Figure 5-11 *Cisco 7975G IP Phone*

With the addition of color and backlighting to the 7965G and 7975G phones comes color and backlighting of the expansion module. The 7916 expansion module attaches to the right side of the phone. Up to two of these modules can be attached to a single phone. The 7915 is also supported for use with the 7965G and 7975G.

Note Neither the 7915 nor 7916 is supported with the 7945G.

Figure 5-12 shows the 7916 expansion module.

Figure 5-12 *Cisco 7916 Expansion Module*

Like its monochrome counterpart, the 7916 has 2 page selector buttons, each providing access to the 12 buttons on the module and attaches to the right side of the phone. The adjustable footstand of the phone has to be removed and replaced with a fixed footstand that supports the form factor of both the phone and the expansion modules. Table 5-6 provides an overview of the features of the 7945G, 7965G, and 7975G phones.

Table 5-6 Cisco 7945G. 7965G, and 7975G IP Phone Features

Feature/ Function	7945G	7965G	7975G
Integrated switch	10/100/1000	10/100/1000	10/100/1000
Display	5-inch 320x240 16-bit color, backlit	5-inch 320x240 16-bit color, backlit	5.6-inch 320x240 16-bit color, backlit touchscreen
Speakerphone	Yes	Yes	Yes
Line keys	2 (lighted)	6 (lighted)	8 (lighted)
Programmable soft keys	4 soft keys, 2 line keys (can be lines, speed dials, or programmable line keys)	4 soft keys, 6 line keys (can be lines, speed dials, or programmable line keys)	5 soft keys, 8 line keys (can be lines, speed dials, or programmable line keys)
Fixed feature keys	10	10	10
Advanced features	High-resolution screen Application integration capabilities Headset hookswitch control	High-resolution screen Application integration capabilities Headset hookswitch control Up to 2 7915 or 7916 expansion modules	High-resolution screen Application integration capabilities Headset hookswitch control Up to 2 7915 or 7916 expansion modules
Hands-free	Yes	Yes	Yes
MWI	Yes	Yes	Yes
XML support	Yes	Yes	Yes
Signaling protocol	SCCP or SIP	SCCP or SIP	SCCP or SIP
802.3af	Yes	Yes	Yes
PoE class	Class 3	Class 3	Class 3
CUCM version	4.1 and later	4.1 and later	4.1 and later

Cisco 8800 Series Phones

Key Topic

The 8800 series is the latest addition to the portfolio. As has been the recurring theme with Cisco's newer series phones, these handsets all use SIP exclusively. They do not

support SCCP. Cisco has introduced some interesting new features in this line. These phones are a new design, from the bottom up, while maintaining a look and feel reminiscent of its predecessors. The lines are sleeker, yet very obviously influenced by the iconic 7900 series phones. They were built with a focus on providing a highly intuitive user experience. Each has been hardware enhanced for high-quality wideband voice and increased echo-cancellation capabilities. In addition, vibration-isolation techniques have been employed on the speakers and microphones to ensure an optimal communication experience.

The 8800 series phones include both audio-only and video-capable models. For video communications with the audio-only models, the Jabber client on the user desktop can be used for video, while the desk phone itself handles the audio. That said, nearly any Cisco IP Phone can be video enabled in this manner.

There are seven phone models in the line, six desktop handset models and one conference room phone model. The series includes the 8811, 8831, 8841, 8851, 8861, 8845, and 8865 phones.

Cisco 8811 IP Phone

The 8811 phone is the entry-level model of the line, but it does not necessarily have the limitations one might assume in an entry-level handset. This phone does have support for headset integration (RJ-9 and AUX ports) and is equipped with a Gigabit Ethernet port/integrated switch. It is a Class 2 PoE device, supporting 802.11af/at power along with Cisco EnergyWise. It also has an integrated Secure Sockets Layer (SSL) virtual private network (VPN) client. This makes it ideal for both knowledge workers and teleworkers alike.

The 8811 is the only model featuring a monochrome display. The display is a 5-inch 800x480 monochrome display with white backlighting. Figure 5-13 shows the 8811 phone.

Figure 5-13 *Cisco 8811 IP Phone*

As shown in the figure, the phone combines soft keys and fixed function keys to keep the most commonly used features at your fingertips. This phone includes 5 line keys (multiple calls per line key), 4 programmable soft keys (context sensitive), a five-way navigation pad, and 12 fixed function keys (Messaging, Directory, Services, Volume, Hold/Resume, Transfer, Conference, Mute, Speakerphone, Headset, End Call, and Return [or backing up one menu level in the phone's menu structure]).

Cisco 8831 IP Phone

The 8831 is purpose built for conference rooms. It consists of a base speaker unit, a wired control panel with dial pad, and up to two microphones. These microphones are available in both wired and wireless configurations. The wireless microphones are rechargeable and come with the charging base. Two 8831 speakers can be daisy-chained together to reach across a large conference table. This avoids the age-old problem of a large table with two conference phones dialed into a meeting. In such meetings, the coordination of muting/unmuting each phone as participants with to speak becomes cumbersome, at best. With the 8831, a single phone can provide 360-degree coverage in the largest conference room. When daisy-chaining speakers, wired microphones must be used. Figure 5-14 shows the 8831 phone.

Figure 5-14 *Cisco 8831 IP Phone*

The 8831 is a full-duplex, wideband audio speakerphone. As with the other models in this series, it is a SIP device. It has a 10/100 Ethernet port for connectivity and is classified as a Class 3 PoE device. The 396x162-pixel monochrome display is white backlit.

The control panel with dial pad has four programmable soft keys and one line key. It also contains fixed feature keys for Volume Control, Mute, Speaker On/Off, and a navigation pad. The base station speaker and microphones each include a mute button as well.

Cisco 8841/8851/8861 IP Phones

These three models are combined into a single section primarily because they look nearly identical. In terms of what is visible from the figures included herein, there is little visible difference, if any, from a frontal view. In fact, the only real difference in appearance from the 8811 is the monochrome display, whereas these three models have color displays. For

that reason alone, front-view pictures of all three models are not included as has been the case up to this point in this chapter. They do have significant feature variation, however. But, first, let's focus on what they have in common. Figure 5-15 shows an 8841 phone.

Figure 5-15 *Cisco 8841 IP Phone*

All three models include a 5-inch high-resolution (800x480) Wide Video Graphics Array (WVGA) color display. None of these, however, are touchscreen displays. The phones have a 10/100/1000 integrated switch and are SIP devices. Again, there is no SCCP support in any of the 8800 series models. Each model has 5 line keys (multiple calls per line key), 4 programmable soft keys (context sensitive), a five-way navigation pad, and 12 fixed function keys (Messaging, Directory, Services, Volume, Hold/Resume, Transfer, Conference, Mute, Speakerphone, Headset, End Call, and Return [for backing up one menu level in the phone's menu structure]).

All the phones support 802.11af/at PoE and Cisco EnergyWise. The similarities come to a somewhat abrupt end there. The 8841 is a Class 2 PoE device, the 8851 is a Class 3 PoE device, and the 8861 is a Class 4 PoE device. The reasons for the differences in power draw are due to newly introduced features and ports on the phone itself. Figure 5-16 shows a rear view of the 8841 phone. This is primarily for reference to illustrate the differences discussed momentarily.

Figure 5-16 *Rear View of the Cisco 8841 IP Phone*

These phones come in either charcoal or white color options. The figure shows the white phone model primarily because the contrast makes the port differences more evident. In Figure 5-16, visible ports include, from left to right, power, network, switch port, AUX, headset, and handset. Also note that there are no ports along the left outer edge of the phone.

The 8851 and 8861 have added Bluetooth functionality in support of a feature known as Intelligent Proximity. Intelligent Proximity for desk phones allows the pairing of the phone to a smartphone. This allows the same functionality at the desk phone as one might see in a modern car with Bluetooth functionality. It will synchronize contacts and call history and provide voice/video connectivity. When the smartphone rings, the desk phone rings along with it and provides answer options. A call in progress can be moved back and forth from the desk phone to the smartphone by selecting a different audio source on the smartphone when a call is in progress. This allows the use of the superior acoustical resources of the desk phone over that of the smartphone.

Another added feature is USB support. The 8851 has one USB port intended for use in charging smartphones. Figure 5-17 shows the rear view of the 8851 phone.

Figure 5-17 *Rear View of the Cisco 8851 IP Phone*

Comparing the figure to Figure 5-16, the only visible difference is the outer left edge where a USB port has been added.

The 8861 has two USB ports. One of those ports, like the 8851, is for smartphone charging; the other is for charging tablets. Figure 5-18 shows the rear view of the 8861 phone.

Figure 5-18 *Rear View of the Cisco 8861 IP Phone*

Like the 8851, the 8861 has the side USB port. But, an additional USB port has been added on the back of the phone as well.

This USB support, on the 8851, 8861, and 8865, is also used in providing support for key expansion modules (KEM). The 8800 KEM has a 4.3–inch, 480x272-pixel, backlit graphical display. The font size has a small and large configuration option for added customization of key labels. The 8851 supports the addition of two KEMs, whereas the 8861 and 8865 support three. The first KEM attaches to the side of the phone using a special interface port and the USB port. Each KEM contains an identical port configuration on both sides. In Figures 5-17 and 5-18, the left outer edge is the KEM connection location. Figure 5-19 shows the 8800 KEM.

Figure 5-19 *Cisco 8800 IP Phone Key Expansion Module*

Each KEM contains 18 physical keys and 2 page keys, for a total of 36 additional keys per module. This means that the addition of KEMs can provide up to an additional 72 line/feature keys for the 8851 and 108 line/feature keys for the 8861 and 8865 phones.

Cisco 8845/8865 IP Phones

The two newest phones in the Cisco IP Phone portfolio are the 8845 and 8865 models. These two models bring integrated 720p HD video to the desk phone. These phones use the same basic form factor as the rest of the 8800 line. However, some modifications make them slightly differ in look, namely the addition of the small camera at the top of the display. This is not an add-on camera, such as that used with the 9971, for example. It is a true

integrated HD camera. The video calling features include a selectable position picture-in-picture (PIP), view swap (remote end or self-view), minimize video, self-view video, and video UI and conference/transfer initiation. There is also a privacy shutter on the integrated camera to stop the video broadcast.

Both models include 10/100/1000 Ethernet capabilities with an integrated switch. Like the 8841/8851/8861 models, these include a 5-inch high-resolution display at 800x480 resolution, 5 line keys, 4 programmable soft keys, and 12 fixed feature keys. Both endpoints also include support for Bluetooth connectivity for headset and Intelligent Proximity pairing to smartphones. This is the same Intelligent Proximity functionality as has been discussed with the 8851 and 8861 phones. Figure 5-20 shows the Cisco 8845 IP Phone.

Figure 5-20 *Cisco 8845 IP Phone*

The 8865 has been enabled with more a somewhat more advanced feature set than the 8845. This includes the addition of USB ports for charging of smartphones (side USB port) and tablets (back USB port) in the same manner as the 8861's configuration. Refer back to Figure 5-18 for the port layout. In addition, the 8865 has been configured to include wireless networking support for 802.11a/b/g/n/ac environments where wired network connectivity may not be available but HD video calling capabilities are desired. In the absence of PoE, a Power Cube 4 is required to power the phone. Another added capability of the 8865 is support for the use of up to three 8800 series KEMs. Figure 5-21 shows the Cisco 8865 IP Phone.

Figure 5-21 *Cisco 8865 IP Phone*

Looking at both Figure 5-20 and Figure 5-21, these phones look nearly identical; however, there are aesthetic differences evident upon closer examination. The 8865 is essentially an 8861 with added video. Both phones, video aside, are identical from a feature perspective. The 8845 does not easily map to its counterpart handset, the 8851, however. The 8845 does include Bluetooth and Intelligent Proximity, but it does not include the USB or KEM support available to the 8851.

Table 5-7 provides an overview of the features of the 8800 series phones.

Table 5-7 Cisco 8800 Series IP Phone Features

Feature/ Function	8811	8831	8841	8851	8861	8845	8865
Integrated switch	10/100/ 1000	N/A	10/100/ 1000	10/100/ 1000	10/100/ 1000	10/100/ 1000	10/100/ 1000
Wireless capability	No	No	No	No	Yes – 802.11a/b/ g/n/ac	No	Yes – 802.11a/b/ g/n/ac

Feature/ Function	8811	8831	8841	8851	8861	8845	8865
Display	5-inch 800x480 backlit mono-chrome		5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color
Speaker-phone	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Line keys	5	1	5	5	5	5	5
Program-mable soft keys	4	4	4	4	4	4	4
Fixed feature keys	12	9	12	12	12	12	12
Integrated video	No	No	No	No	No	Yes – 720p HD, H.264 AVC, 80-deg FoV, privacy shutter	Yes – 720p HD, H.264 AVC, 80-deg FoV, 25-deg vertical tilt, privacy shutter
Advanced features	Gig Ethernet, wideband audio	Wired or wireless micro-phone kit, daisy-chain configura-tion	Gig Ethernet, wideband audio	Intelligent Proximity (Bluetooth hands-free pairing with smart-phone), USB smart-phone charging	Intelligent Proximity (Bluetooth hands-free pairing with smart-phone), USB smart-phone and tablet charging	Intelligent Proximity (Bluetooth hands-free pairing with smart-phone),	Intelligent Proximity (Bluetooth hands-free pairing with smartphone), USB smartphone and tablet charging
Hands-free	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MWI	Yes	No	Yes	Yes	Yes	Yes	Yes

Feature/ Function	8811	8831	8841	8851	8861	8845	8865
XML support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Signaling protocol	SIP	SIP	SIP	SIP	SIP	SIP	SIP
802.3af	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PoE class	Class 2	Class 3	Class 2	Class 3	Class 4	Class 2	Class 4
CUCM version	8.5(1) and later	7.1(5) and later	8.5(1) and later	8.5(1) and later	8.5(1) and later	CUCM: 8.5.1 (nonsecured mode), 8.6.2, 9.1.2, 10.0 and later Bus. Edition: 8.6.2, 9.1.2, 10.0 and later HCS: 8.6.2 and later	CUCM: 8.5.1 (nonsecured mode), 8.6.2, 9.1.2, 10.0 and later Bus. Edition: 8.6.2, 9.1.2, 10.0 and later HCS: 8.6.2 and later

Cisco 8900 Series Phones

Key Topic

The 8900 series phones were created to allow businesses to begin moving video communications to the desktop of all users. These phones are general business collaboration endpoints intended for all types of users. Two phone models are currently available in the 8900 series line: the 8945 and 8961.

Cisco 8945 IP Phone

The 8945 phone is a collaborative meeting endpoint delivering standard definition video to the desktop via an integrated Video Graphics Array (VGA) (640x480) video camera. It supports standard H.264 video at frame rates of up to 30 frames per second (fps). It includes a 5-inch thin-film transistor (TFT) color display. The color backlit display runs a resolution of 640x480 pixels and has an antiglare finish. Figure 5-22 shows the 8945 IP Phone.

Figure 5-22 *Cisco 8945 IP Phone*

The 8945 includes 4 tricolor LED line/feature keys, 4 programmable soft keys, and 12 fixed function keys. The fixed function keys include Applications, Directories, Messages, Volume Control, Headset, Speakerphone, Audio Mute, Video Mute, Transfer, Conference, Redial, and Hold/Resume. As an added feature, Bluetooth support has been built in to this model for use with hands-free headsets. However, unlike the 8851/8861, the Bluetooth support on this model does not have Intelligent Proximity.

The body of the 8945 is built from reground and recycled plastics, making this an eco-friendly and rugged phone. A Class 3 PoE device, the 8945 has a 10/100/1000 integrated switch and supports both SCCP and SIP for line-side signaling. Adding to its green capabilities is a deep sleep option, which cuts the power consumption down to less than 1 watt during off-hours.

Cisco 8961 IP Phone

The 8961 is a collaboration endpoint intended for use by knowledge workers, managers, and executives desiring desktop voice communication capabilities. Designed with ergonomics in mind, the 8961 has clean, uncluttered lines and an intuitive user interface. The 5-inch

640x480-pixel TFT display is backlit and has an antiglare finish and an adjustable viewing angle. It is designed to enhance the user experience when using multimedia applications, such as XML or MIDlet applications developed both by Cisco and by third-party developers. Figure 5-23 shows the 8961 IP Phone.

Figure 5-23 *Cisco 8961 IP Phone*

This phone features 5 programmable line/feature keys, 4 programmable soft keys, and 12 fixed feature keys. It has an integrated 10/100/1000 switch built in. The 8961 supports only SIP for line-side signaling and is classified as a Class 4 PoE device. It has a USB port for use with wired headsets or the base station of wireless headsets.

Like the 8945, the 8961 is manufactured from reground/recycled plastics. It also supports the deep sleep mode feature for off-hours power saving. It also supports Cisco EnergyWise implementations.

The 8961 uses the Cisco Unified IP KEM; however, unlike the previously discussed phone models, only one KEM can be attached to this phone. Figure 5-24 shows the KEM for the 8961 phone. This same KEM is also used with the 9900 series phones, discussed in the next section.

Figure 5-24 *Cisco Unified IP Key Expansion Module*

The KEM has 18 tricolor LED buttons for lines/features and 2 page buttons, adding a total of 36 additional line/feature buttons to the phone's capacity. The KEM has a 480x272-pixel color, backlit, antiglare display. It is line-powered when the phone is using 802.3AT PoE or can be powered by a Power Cube 4 external power supply. Table 5-8 provides an overview of the features of the 8900 series phones.

Table 5-8 Cisco 8900 Series IP Phone Features

Feature/Function	8945	8961
Integrated switch	10/100/1000	10/100/1000
Display	5-inch 640x480 TFT, 24-bit color	5-inch 640x480 TFT, 24-bit color
Speakerphone	Yes	Yes
Line keys	4	5
Programmable soft keys	4	4

Feature/Function	8945	8961
Fixed feature keys	13	12
Advanced features	Integrated camera, Bluetooth for headset connection	Gigabit Ethernet, wideband audio, XML/MIDlet support
Hands-free	Yes	Yes
MWI	Yes	Yes
XML support	Yes	Yes
Signaling protocol	SCCP or SIP	SIP
802.3af	Yes	Yes
PoE class	Class 2	Class 4
CUCM version	7.1(5) and later	7.1(3) and later

Cisco 9900 Series Phones

Key Topic

Building upon the features offered in the 8961 phone, the 9900 series adds desktop video support with the inclusion of a USB-connected video camera. Like the 8961, the 9900 series phones are SIP endpoints only. They do not support SCCP. The 9900 series phones deliver high-quality audio, standard-definition video and support for an extensive array of XML and MIDlet applications. This makes them ideal for knowledge workers, managers, and executives desiring a higher-end multimedia communication experience. The compact video camera mounts directly onto the phone's display. The display tilt is adjustable, as is that of the camera. There is also a physical shutter that can be opened and closed based on the user's preference. The camera is capable of encoding 30 frames per second (fps) at 352x288 Common Intermediate Format (CIF) resolution or 24 fps at 640x480 VGA resolution (H.264). The phone models in this series include the 9951 and 9971. Both are class 4 PoE devices. However, these phones have a deep sleep feature that drops their power consumption by over 90 percent during off-hours.

Cisco 9951 IP Phone

The 9951's 5-inch, 24-bit, 640x480-pixel TFT display is backlit and has an antiglare finish and an adjustable viewing angle. The display supports the use of both left-to-right and right-to-left language deployments as needed in global deployments. It has ten tricolor LED keys arrayed in two columns of five on either side of the display. Five of these keys are programmable for use with telephony functions such as line keys, speed dials, BLF, call park, call forward, and so on. The other five keys are session keys, which can be tied to applications, services, or other similar functions. Figure 5-25 shows the 9951 IP Phone.

Figure 5-25 *Cisco 9951 IP Phone*

There are also 4 programmable soft keys in a row just beneath the display as well as 12 fixed-function feature keys on the phone itself, arrayed around the keypad. Additional features added to the 9951 phone include support for Bluetooth 2.0 for wireless headset support. Two USB ports are also on board for use with wired headsets. Whether wired or wireless, the phone supports high-definition voice for increased sound clarity. The 9951 includes an integrated 10/100/1000 switch port to facilitate the connection of a wired workstation to the phone. This phone does support the use of XML-based applications and services and the use of up to three KEMs. The first KEM is powered via the PoE provided by the access layer switch. Additional KEMs require the use of external power.

Cisco 9971 IP Phone

The 9971's 5.6-inch, 24-bit, 640x480-pixel TFT display is backlit and has an antiglare finish and an adjustable viewing angle. Unlike the display of the 9951, the 9971 display is a touch-screen. The display supports the use of both left-to-right and right-to-left language deployments as needed in global deployments. It has 12 tricolor LED keys arrayed in 2 columns of 6 on either side of the display. Six of these keys are programmable for use with telephony functions such as line keys, speed dials, BLF, call park, call forward, and so on. The other 6 keys are session keys that can be tied to applications, services, or other similar functions. Figure 5-26 shows the 9971 IP Phone.

Figure 5-26 *Cisco 9971 IP Phone*

Like its 9951 smaller counterpart, the 9971 phone includes support for Bluetooth 2.0 for wireless headset support. Two USB ports are also on board for use with wired headsets. Whether wired or wireless, the phone supports high-definition voice for increased sound clarity. The 9971 includes an integrated 10/100/1000 switch port to facilitate the connection of a wired workstation to the phone.

The 9971 extends the functionality of the 9951 with an additional line and session key and the addition of an 802.11 a/b/g wireless network radio. Note that when the phone is deployed wirelessly, the integrated 10/100/1000 switch port cannot be used.

This phone does support the use of XML-based applications and services and the use of up to three KEMs. The first one is powered via 802.3AT PoE provided by the access layer switch. Additional KEMs require the use of external power. Table 5-9 provides an overview of the features of the 9900 series phones.

Table 5-9 Cisco 9900 Series IP Phone Features

Feature/Function	9951	9971
Integrated switch	10/100/1000	10/100/1000
Display	5-inch 640x480 TFT, 24-bit color	5.6-inch 640x480 TFT, 24-bit color
Speakerphone	Yes	Yes
Line/session keys	10	12

Feature/Function	9951	9971
Programmable soft keys	4	4
Fixed feature keys	12	12
Advanced features	H.264 video, Bluetooth for headset, USB for headset, KEM support	H.264 video, Bluetooth for headset, USB for headset, KEM support, Wi-Fi
Hands-free	Yes	Yes
MWI	Yes	Yes
XML support	Yes	Yes
Signaling protocol	SIP	SIP
802.3af	Yes	Yes
PoE class	Class 4	Class 4
CUCM version	7.1(3)su1 and later	7.1(3)su1 and later

Cisco Collaboration Desktop Endpoints

Cisco has made significant changes in the realm of collaboration by advancing innovation and reducing cost of deployment. The overarching goal is to provide a rich communication experience to users at all levels on all devices, regardless of their manufacturer or operating system. The first steps on this path commenced through the formation a partnership with, followed soon thereafter by the acquisition of, TANDBERG.

The TANDBERG acquisition brought with it extensive video infrastructure, endpoints, and technologies. This section focuses on endpoints, both acquired and newly created. The EX60 and EX90 endpoints were not alone in TANDBERG's portfolio, certainly. However, the evolutionary path of Cisco video endpoint technologies has seen those other endpoints fade away into the past. The newest line of endpoints are focused on the desktop experience. Hence, they are designated with at DX moniker.

Cisco EX60

The EX60 is meant to be an all-in-one collaboration device by enabling a personalized face-to-face communication and content-sharing experience. Although it is primarily a video endpoint, it can be used for audio-only calls as well. It supports numeric, IP address, and SIP Universal Resource Identifier (URI) dialing functions. It does include an integrated 10/100/1000 switch to facilitate both network and workstation connectivity via a single network drop.

Its 21.5-inch HD display is capable of 1920x1080 resolution and 5-ms response time and provides a 170-degree viewing angle. As a video communications endpoint, it supports resolutions of 1080p30 and 720p60. The tilt of the unit can be adjusted within the range of 5 to

15 degrees from vertical. The accompanying TelePresence Touch 8 pad allows for simple, intuitive operation of the endpoint. In the spirit of providing a face-to-face communication experience, the unit includes an integrated microphone along with two speakers built in to the front of the display panel. It also includes a handset for times when private audio communication is desired. The use of an external headset and microphone is also supported via 3.5-mm jacks built in to the unit.

The EX60 includes a TelePresence PrecisionHD camera that can be used as a document camera by moving it to point straight down. When it detects that it is being moved into vertical position, it flips the picture so that both parties see the document right-side up. The camera also has a privacy shutter built in to the bezel. This allows the local user to control whether the far end can see him/her. It is the video equivalent of an Audio Mute button. The camera has a 1/3-inch 2.1-megapixel sensor, allowing a 50-degree horizontal / 29-degree vertical field of view.

Beginning with Cisco Unified Communications Manager 8.6, the EX60 can be registered as a SIP endpoint in a similar fashion to any other Cisco IP Phone. This was a crucial step in merging the legacy TANDBERG Video Communications Server (VCS) architecture with the vision and future of a single Cisco collaboration call control foundation. Although the endpoint can be used with either VCS or CUCM, future development efforts will be primarily focused on CUCM-related functionality. Figure 5-27 shows the Cisco TelePresence EX60.

Figure 5-27 *Cisco TelePresence EX60*

Regardless of deployment model, the EX60 supports H.261, H.263, H.263+, and H.264 video standards. When it is not filling its role as a video endpoint, it can serve as a nicely sized second monitor for a single DVI-I attached workstation or laptop. Through this connection, content can be shared into the video stream at 720p.

The EX60 is supported with Cisco TelePresence Version TC4.0 and later or TE6.0.

Cisco EX90

The EX90 is really the big brother to the EX60. In both form and function, it is quite evident that they share a common ancestry. Like the EX60, the EX90 includes an integrated 10/100/1000 switch to facilitate both network and workstation connectivity via a single network drop.

It has a 24-inch HD display capable of 1920x1200 resolution and 5-ms response time, and provides a 160-degree viewing angle. As a video communications endpoint, it supports resolutions of 1080p30 and 720p60. The tilt of the unit can be adjusted within the range of 5 to 15 degrees from vertical. The accompanying TelePresence Touch 8 pad allows for simple, intuitive operation of the endpoint. In addition to the integrated microphone and dual front speakers, the EX90 also has a built-in subwoofer for higher sound quality. It also includes a handset for times when private audio communication is desired. The use of an external headset and microphone is also supported via the dual USB ports or 3.5-mm jacks built in to the unit.

The EX90 includes a TelePresence PrecisionHD camera that can be used as a document camera by moving it to point straight down. When it detects that it is being moved into vertical position, it flips the picture so that both parties see the document right-side up. The camera also has a privacy shutter built in to the bezel.

Unlike the EX60, the EX90 has an optical, motorized zoom feature. The camera has a 1/3-inch 2.1-megapixel sensor, allowing a 45- to 65-degree horizontal / 40- to 27-degree vertical field of view, depending on the zoom factor.

Another key difference between the EX60 and EX90 is support for a feature known as multisite. EX60 does not support it, whereas EX90 does. This feature is enabled through the addition of an option key in the TC code. Like the EX60, beginning with CUCM 8.6, the EX90 can be registered as a SIP endpoint. As mentioned, while the endpoint can be used with either VCS or CUCM, future development efforts will be primarily focused on CUCM-related functionality. Figure 5-28 shows the Cisco TelePresence EX90 used in an education setting.

Figure 5-28 *Cisco TelePresence EX90*

Regardless of deployment model, the EX90 supports H.261, H.263, H.263+, and H.264 video standards. As with its counterpart, it can serve as a nicely sized second monitor for a DVI-I or HDMI attached workstation or laptop. Through this connection, content can be shared into the video stream at 1080p. The EX90 also has additional capabilities including HDMI in, HDMI out (dual display option), as well as audio in/audio out (3.5-mm jack on rear panel).

The EX90 is supported with Cisco TelePresence software version TC3.1 and later or TE6.0. Table 5-10 provides an overview of the features of the Cisco EX Series Endpoints.

Table 5-10 Cisco EX Series Endpoint Features

Feature/Function	EX60	EX90
Integrated switch	10/100/1000	10/100/1000
Display	21.5-inch LCD with LED backlight, 1920x1080, 170-degree viewing angle, 5-ms response	24-inch LCD with LED backlight, 1920x1200, 160-degree viewing angle, 5-ms response
Speakerphone	Yes	Yes
Camera	PrecisionHD, privacy shutter, document camera mode, 1/3-inch 2.1 mp, 50-degree horizontal / 29-degree vertical field of view	PrecisionHD, privacy shutter, document camera mode, optical motorized zoom, 1/3-inch 2.1 mp, 45-to 65-degree horizontal / 40- to 27-degree vertical field of view
Video standards	H.261 H.263 H.263+ H.264	H.261 H.263 H.263+ H.264

Feature/Function	EX60	EX90
Resolution	1920x1080 (16:9)	1920x1200 (16:10)
Signaling protocol	CUCM: SIP VCS: SIP/H.323	CUCM: SIP VCS: SIP/H.323
TelePresence software version	TC4.0 or TE6.0	TC3.1 or TE6.0
CUCM version	8.6(2) and later	8.6(2) and later

Cisco DX650

The Cisco Desktop Experience line of endpoints began with the DX650. Two additional endpoints have subsequently been added to the line: DX70 and DX80. Only the DX650 is covered at this time.

The DX650 is an Android OS (Jellybean)-based collaboration endpoint with a 7–inch, backlit, widescreen Super Video Graphics Array (WSVGA) capacitive touchscreen LCD with 1024x600 pixel resolution. The display can tilt between 5 degrees forward to 25 degrees backward to allow for the optimal viewing angle. An integrated 1080p capable camera, with privacy shutter, is also included. The camera has a 75-degree vertical / 67.4-degree horizontal field of view.

It supports HD voice and video communications, as well as an extensive list of applications. This includes Cisco applications, such as Jabber IM and Presence, WebEx Meetings, and more, in addition to applications available on the Google Play Store, such as Pandora, Netflix, and yes, Angry Birds. Access to these applications can be tightly controlled via the CUCM administration web application. Figure 5-29 shows the Cisco DX650.

Figure 5-29 *Cisco DX650*

First and foremost, the DX650 is a SIP-based collaboration endpoint. It has a visual telephony and messaging interface, favorites list right on the desktop, and the ability to perform directory searches. It supports both numeric and URI dialing features.

HD video support includes H.264 and advanced video coding (AVC) up to 1080p30.

The DX650 can be used in both wired and wireless environments. It includes a 10/100/1000 integrated switch for wired connections. For wireless connections, it has an 802.11a/b/g/n-capable radio built in. Bluetooth support is also built in to this device. The functionality is not simply for headset use, although it works very well with a variety of available models. An additional feature known as Intelligent Proximity for Mobile Voice allows a paired smartphone to make use of the superior audio capabilities of the DX650 for calls to and from that phone. Contacts and call histories can be synchronized into the DX650 as well to provide a more seamless experience.

The use of external displays is encouraged with the DX650. It has an HDMI port and a display port for external display connectivity. In addition, it has two standard USB (type A) ports for keyboard/mouse/flash drive, and so on connectivity and one micro-USB port.

The DX650 is PoE capable and is a Class 3 device with 802.3af power or class 4 device with 802.3at power. The difference really comes down to what types of devices need to be powered by the USB ports. If higher-power devices are connected, the DX650 must pull more power from the switch.

The DX650 comes with the Cisco AnyConnect VPN client embedded; however, it is also compatible with the Cisco mobile and remote-access (a.k.a. collaboration edge) architecture for VPN-less connectivity. Obviously, this access requires a CUCM version capable of supporting that architecture (9.x and later). Otherwise, the DX650 is supported in CUCM 7.1(5) and later. Table 5-11 provides an overview of the features of the DX650.

Table 5-11 Cisco DX650 Features

Feature/Function	DX650
Integrated switch	10/100/1000
Display	7-inch diagonal, backlit WSVGA capacitive touchscreen LCD with 1024x600-pixel resolution
Speakerphone	Yes
Camera	1080p, privacy shutter, 75-degree vertical / 67.4-degree horizontal field of view
Video standards	SIP only H.264 AVC
Resolution	WSVGA 1024x600
Signaling protocol	SIP
CUCM version	7.1(5) and later

Cisco Jabber Software Clients

Key Topic

Cisco Jabber has come a very long way in a relatively short time. It represents the evolutionary result of a number of prior clients including Cisco IP Communicator (CIPC), Cisco Unified Personal Communicator (CUPC), WebEx Messenger, TANDBERG Movi, and numerous other components. It has become the all-in-one client we have so long desired in the Cisco collaboration realm.

Cisco Jabber offers one common user experience across multiple platforms, including desktops, tablets, and smartphones. It has the same look and feel regardless of whether it is used on a Windows platform, Apple OS X / IOS platform, Android platform, or web platform. The fact that it is based on a unified Client Services Framework (CSF) allows it to layer multiple services into a single, highly flexible platform. On the desktop client, multiple custom tabs can be added to provide access to frequently used websites, widgets, and applications. The Jabber software development kit (SDK) provides the ability to fully customize the client look, feel, and content. Regardless of platform, when launched, the client kicks off a service discovery process.

Cisco Jabber for Desktop

For desktops, Cisco Jabber supports both Windows and Mac operating systems. The look and feel of each client, while nearly identical, will take on the attributes expected in the OS in which each is used. Jabber includes cloud-based or premise-based instant messaging (IM), presence, voice, HD video, voice messaging, desktop sharing/remote control, and conferencing capabilities all from a single client. It also integrates with Microsoft Office applications for presence status, calendar information, and communication from within the Office application.

Being a multiuse client, Jabber makes use of a number of protocols to facilitate communications. For IM, Jabber makes use of standard extensible messaging and presence protocol (XMPP). Being such, Cisco IM&P services can be easily federated with any other standards-based Extensible Messaging and Presence Protocol (XMPP) implementation. For voice and video calling capabilities, Jabber is a SIP-based endpoint. It can operate in soft phone mode, providing full calling capabilities right from the desktop. This is useful when there is no desk phone present on the desktop or when the end user is on the move. When a desk phone is available, Jabber can integrate with it through the use of Computer Telephony Integration (CTI). This allows the client to make use of the desk phone for communications launched from the Jabber client itself. It also allows the ability to enable video communications for any Cisco IP Phone. All that is required on the workstation is a webcam. Jabber will make use of the webcam for video while using the desk phone for audio. For video calls, Jabber is capable of resolutions up to 720p30 when expanded to full-screen mode. It does support SIP URI dialing as well as traditional numeric dialing. For multiparty calls, a video or audio conferencing resource is required as appropriate for the call. Figure 5-30 shows the Cisco Jabber for Windows client.

Figure 5-30 *Cisco Jabber for Windows*

For comparison, Figure 5-31 shows the Cisco Jabber for Mac client.

Figure 5-31 *Cisco Jabber for Mac*

In viewing both Figure 5-30 and Figure 5-31, it becomes evident that these two clients present a common user experience even though they are running on top of two very different platforms. Each has the characteristic aesthetic traits of the OS, but identical in form and function otherwise. The same holds true for Jabber on all supported platforms.

Desktop sharing can be initiated from the client as well simply by initiating an IM session. The client can be in either desk phone mode or soft phone mode when the share is initiated. The share can also be used to control the desktop being shared. In cases where the screen share is initiated from a multiparty IM session, the screen share can include up to five participants. No call need be active between the two endpoints. If only an IM session is active, the screen share is initiated via XMPP. If a call is active, the share is initiated via Binary

Floor Control Protocol (BFCP). This is a relatively new addition, however, in Jabber 10.5 and later. Note that that IM-only screen share is using Remote Desktop Protocol (RDP) to accomplish the connection. Therefore, it is available only with Jabber for Windows.

Prior to Jabber 10.5, only BFCP was used for desktop share, and no remote control capability was possible. This necessitated the need for the Jabber client to be in soft phone mode and a call to be up between the desktops to initiate the share. This is no longer the case. But, it is useful to understand the history for a number of reasons, potential exam coverage included.

Cisco Jabber for Tablet

Cisco Jabber for iPad and Android enable mobile users to make use of Jabber on a mobile platform somewhat larger than the smartphone and more portable than even the smallest laptop computer. Tablets have taken over as the perfect balance of application portability and screen real estate. It is only natural that they become an extension of our work desktop. Using the Jabber client enables the full collaboration experience in a very small footprint. This includes IM, presence, voice, HD video, content sharing, and so on. It will run on iPad, iPad mini, or an Android tablet. Figure 5-32 shows the Cisco Jabber for iPad client.

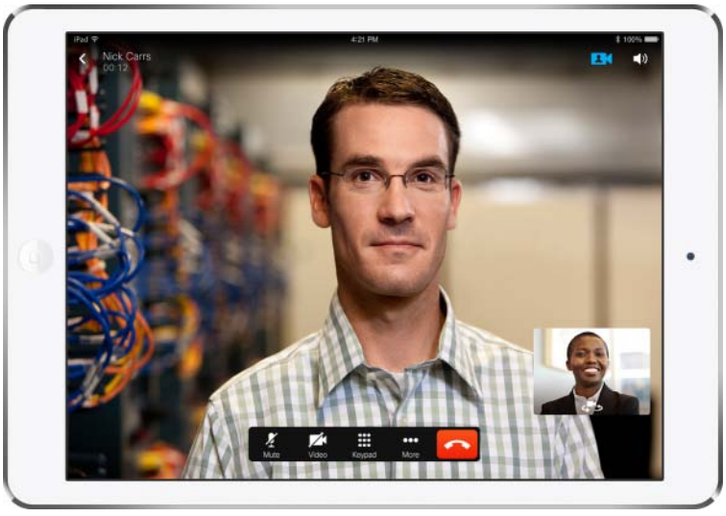


Figure 5-32 *Cisco Jabber for iPad*

Figure 5-32 shows the video call layout with picture-in-picture and call controls. During a video call, the camera in use can be switched from forward to rear and back at will. For comparison, and to show a slightly different view of Jabber's functionality, Figure 5-33 shows the Jabber for Android client running on a tablet.

Figure 5-33 shows the Jabber client contacts and IM screen. The Jabber client on both platforms has the same look, feel, and capabilities. The quality of video will, of course, be subject to the wireless network radio, processor and optics capabilities of the tablet. For example, the quality of the experience on a new iPad Air with Retina camera and display will be superior to that on an iPad 3 without Retina capabilities.

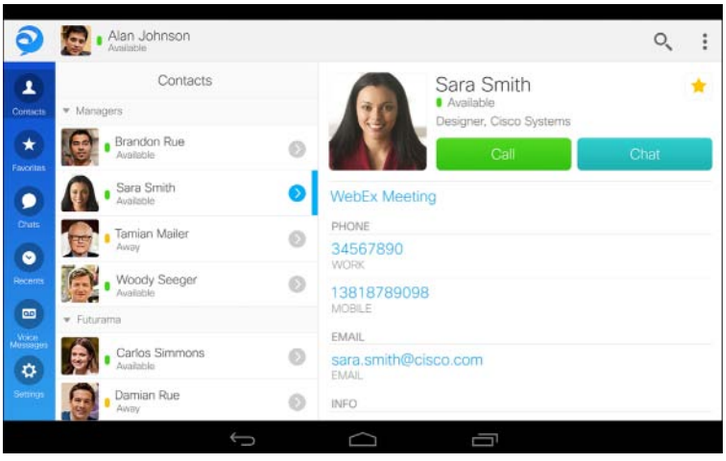


Figure 5-33 *Cisco Jabber for Android on Tablet*

5

Cisco Jabber for Smartphone

On the smartphone front, the Jabber client runs on the iPhone and Android platforms. Like the tablet versions, the smartphone versions will support IM, presence, voice, and HD video. Again, the video quality is subject to hardware capabilities. Figure 5-34 shows the Jabber for iPhone client.

Figure 5-34 *Cisco Jabber for iPhone*

Figure 5-34 shows the control console on the client. Figure 5-35 shows the Jabber for Android client on a smartphone. Again, the clients have the same look, feel, and capabilities. The difference in the two figures is merely to show differing views of the Jabber client capabilities.

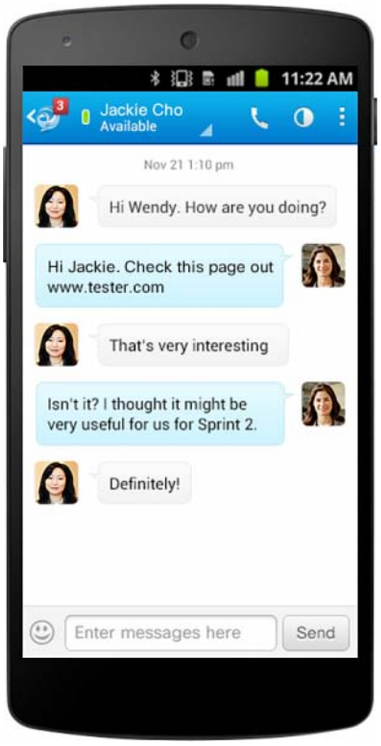


Figure 5-35 *Cisco Jabber for Android on Smartphone*

Figure 5-35 shows an IM session in progress on the Jabber client. Notice the escalation icons at the top of the client. These function identically to the escalation functions on the tablet and desktop clients.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 5-12 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 5-12 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
Section	Cisco 7800 series phones	84
Section	Cisco 8800 series phones	95
Section	Cisco 8900 series phones	105
Section	Cisco 9900 series phones	109
Section	Cisco collaboration desktop endpoints	112
Section	Cisco Jabber software clients	118

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

720p30, 720p60, 1080p30, 802.3af PoE, 802.3at PoE, 802.11a/b/g/n/ac, Binary Floor Control Protocol (BFCP), Computer Telephony Integration (CTI), instant messaging (IM), key expansion module (KEM), Remote Desktop Protocol (RDP), Skinny Call Control Protocol (SCCP), software development kit (SDK), Session Initiation Protocol (SIP), Universal Resource Identifier (URI), Extensible Messaging and Presence Protocol (XMPP)

This chapter covers the following topics:

- **Cisco Collaboration Endpoint Protocol Overview:** This section takes a look at the protocols in use for line-side signaling with Cisco collaboration endpoints.
- **Cisco IP Phone Configuration:** This section discusses the configuration requirements and options for Cisco IP Phones in Cisco Unified Communications Manager.
- **Cisco IP Phone Registration Process:** This section covers the boot and registration process of Cisco IP Phones.
- **Cisco Jabber Configuration:** This section examines configuration requirements and options for Cisco Jabber in Cisco Unified Communications Manager.
- C**isco Jabber Installation and Registration Process:** This section examines the parameters and methodology used in installing Cisco Jabber and the processes used in registering it with Cisco Unified Communications Manager.
- **Cisco Jabber Installation and Registration Process:** This section describes the available tools to help verify status of Cisco IP Phones and Cisco Jabber.

CHAPTER 6

Configuring Cisco Unified IP Phones and Cisco Jabber

This chapter discusses the configuration of the Cisco IP Phone models referenced on the exam blueprint and also discusses Cisco Jabber. Chapter 5, "Cisco IP Phones, Desk Endpoints, and Jabber Overview," discussed a wider array of the overall Cisco IP Phone portfolio. Cisco IP Phone configuration does not vary by a significant degree from model to model across the IP Phone portfolio. That said, this chapter touches on the line-side protocols in use, the IP Phone boot and registration process, general configuration parameters, and status verification mechanisms available for the phones. In addition, the discussion delves into the configuration of Cisco Jabber. The focus remains primarily on the client configuration options. However, some discussion of server-side parameters is required on a number of fronts, including the Cisco Unified Communications Manager (CUCM) service profiles and Domain Name System (DNS) records necessary for Jabber to discover services and function properly.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 6-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 6-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco Collaboration Endpoint Protocol Overview	1–2
Cisco IP Phone Configuration	3–7
Cisco IP Phone Registration Process	8–11
Cisco Jabber Configuration	12–14
Cisco Jabber Installation and Registration Process	15–18
Cisco Collaboration Endpoint Status Verification	19–20

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which protocols are Cisco proprietary?

   a. CDP
   b. LLDP-MED
   c. SIP
   d. SCCP

2. Which protocols are used by Cisco collaboration endpoints to download their configuration files?

   a. SIP
   b. LDAP
   c. TFTP
   d. HTTP

3. Which of the following is the primary means by which an endpoint is uniquely identified in CUCM?

   a. TFTP Option 150
   b. IP address
   c. MAC address
   d. DNS

4. Which of the following must be configured for auto-registration to function?

   a. Universal device and line templates
   b. Calling search spaces
   c. TAPS
   d. Self-Provisioning

5. When a DX650 requires a firmware upgrade, which of the following will occur?

   a. It will download at next phone reset. The phone will be unusable during upgrade.
   b. It will download in the background, not interfering with phone operation.
   c. It will prompt the user to allow the download.
   d. It will wait until an administrator schedules a bulk update.

6. Which of the following has to be changed on a Cisco IP Phone to statically configure the TFTP server address?

   a. Alternate TFTP set to yes
   b. Static IP address
   c. DHCP set to no
   d. Phone to use SCCP

7. Video capabilities on CUCM registered phones can be enabled globally in which of the following pages?

   a. Enterprise Parameters
   b. CallManager Service Parameters
   c. Enterprise Phone Parameters
   d. Cisco Unified CM

8. Cisco inline power was replaced by which IEEE standard?

   a. 802.3at
   b. 802.3af
   c. 802.11n
   d. 802.11ac

9. Which protocols can provide the voice VLAN ID to the phone at boot?

   a. DHCP
   b. TFTP
   c. CDP
   d. LLDP-MED

10. What parameter is added to the DHCP scope for the voice VLAN?

    a. Address reservation
    b. DHCPOFFER
    c. Option 150
    d. DHCPDISCOVER

11. What is the configuration filename requested from the TFTP server by an IP Phone with a MAC address of 000C1ACE0511?

    a. SEP000C1ACE0511.cnf.xml
    b. SIP000C1ACE0511.cnf.xml
    c. SAP000C1ACE0511.cnf.xml
    d. CMDefault.cnf.xml

12. Which Jabber deployment mode offers the most limited feature set?

    a. Full UC mode
    b. IM only mode
    c. Phone mode
    d. Windows mode

13. Jabber users are identified by which of the following?

    a. CUCM DN
    b. LDAP username
    c. AD username
    d. JID

14. With all users in full UC mode, how many users can a single IM&P server support?

    a. 40,000
    b. 10,000
    c. 15,000
    d. 45,000

15. Which of the following options will result in Jabber registering with CUCM?

    a. Selecting Use My Computer for Calls in the Jabber client
    b. Selecting Use My Desk Phone for Calls in the Jabber client
    c. No need because it always registers with CUCM as an endpoint
    d. Selecting Disable Phone Services in the Jabber client

16. When outside of the network, Cisco Jabber uses which of the following DNS SRV records to complete service discovery and reach domain.com?

    a. _cuplogin._tcp.domain.com DNS SRV record
    b. _xmpp-server._tcp.domain.com DNS SRV record
    c. _cisco-uds._tcp.domain.com DNS SRV record
    d. _collab-edge._tls.domain.com DNS SRV record

17. When inside the network, Cisco Jabber uses which of the following to complete service discovery and reach domain.com?

    a. _cuplogin._tcp.domain.com DNS SRV record
    b. _xmpp-server._tcp.domain.com DNS SRV record
    c. _xmpp-client._tcp.domain.com DNS SRV record
    d. _collab-edge._tls.domain.com DNS SRV record

18. Which must be configured in CUCM for Jabber clients to function properly in full UC mode?

- **a.** UC service profile
- **b.** TFTP server
- **c.** CTI route point
- **d.** Auto-registration

19. The Phone Status screen on a 9971 IP Phone shows all but which of the following?

- **a.** Active CUCM node
- **b.** Active load version
- **c.** Inactive load version
- **d.** Model number

20. Which status screen displays jitter experience during a call?

- **a.** Status Messages
- **b.** Call Statistics
- **c.** Ethernet Statistics
- **d.** Wireless Statistics

Foundation Topics

Cisco Collaboration Endpoint Protocol Overview

A protocol, generally defined, is merely a set of rules for a given scenario or situation. In the medical field, a protocol is a specific set of steps that must be followed to ensure proper, consistent patient care. In social settings, protocol is known more commonly as etiquette. No matter how you view it, protocol is an agreed upon manner of behavior for a given scenario.

In this case, the protocols relevant to this discussion are the rules dealing specifically with the need to provide a means of communication between call control and endpoints. To facilitate said communication, additional protocols are required in the underlying infrastructure. TCP/IP is one of those, certainly. But, this book is not about TCP/IP, specifically. That said, some aspects and underlying components of the larger TCP/IP suite of protocols are relevant. The protocols associated specifically with Cisco collaboration architectures are rather numerous. Those relevant to the discussions within this book, and certainly within this chapter, are not quite so numerous. There are protocols specific to discovery and information relay. There are protocols specific to IP addressing and file transfer. The list includes the following:

- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED)
- Dynamic Host Control Protocol (DHCP)
- Trivial File Transfer Protocol (TFTP)
- Hypertext Transfer Protocol (HTTP)
- Skinny Client Control Protocol (SCCP)
- Session Initiation Protocol (SIP)
- Real-time Transport Protocol (RTP)
- Secure Real-time Transport Protocol (SRTP)
- Simple Object Access Protocol (SOAP)
- Extensible Messaging and Presence Protocol (XMPP)
- Lightweight Directory Access Protocol (LDAP)
- Computer Telephony Interface (CTI)
- Computer Telephony Interface Quick Buffer Encoding (CTIQBE)
- Cisco Audio Session Tunnel (CAST)
- Internet Message Access Protocol (IMAP)

Table 6-2 details the protocols of particular relevance to Cisco collaboration endpoints.

Key Topic

Table 6-2 Protocols Used by Cisco Collaboration Endpoints

Protocol	Description
CDP	Cisco proprietary protocol created in 1994 to provide a mechanism for management systems to automatically learn about devices connected to the network. Endpoints use CDP to communicate with the LAN switch regarding the ID of the voice/video VLAN, per-port power management details, and quality of service (QoS) information.
LLDP-MED	An IEEE standard protocol built specifically for voice applications. LLDP-MED is an extension of LLDP. It defines how a switch transitions from LLDP to LLDP-MED if an endpoint is detected. LLDP-MED is closely related to CDP and contains similar features and functions. LLDP-MED reports VLAN and power information but contains the ability to specify additional capabilities beyond those reported by CDP.
DHCP	Dynamically allocates IP address information to clients requesting it. Basic information includes IP address, subnet mask, default gateway, and default gateway. For collaboration endpoints, the DHCP server also provides the Option 150 TFTP server address with which the endpoint needs to make contact to download its configuration and firmware.
TFTP	A User Datagram Protocol (UDP)-based file transfer protocol that requires no authentication. Cisco IP Phones use TFTP to download their firmware and configuration files. The address of the server is provided to the endpoint by the DHCP Option 150 parameter in the DHCP scope for the voice/video VLAN.
HTTP	Typically associated with web services, HTTP can be used by newer endpoints to download configuration information and firmware in a similar fashion as is done with TFTP. IP Phones upgrade their firmware images using HTTP on port 6970 from TFTP services integrated into one or more call processing platforms. When HTTP is not available, the phones use TFTP.
SCCP	Cisco proprietary signaling protocol used in the absence of a feature-rich industry standard alternative. SCCP works only between Cisco IP Phones and CUCM. Now that SIP has finally reached feature parity, SCCP is slowly being phased out.
SIP	Industry-standard (IETF) signaling protocol used in both line-side and trunk-side signaling communications. Nearly all Cisco IP Phones support SIP as the line-side signaling protocol. Many of the newer endpoints support only SIP.
RTP	A standard, UDP-based protocol used for the transport of real-time media traffic (voice and video).
SRTP	An extension to RTP meant to provide it with encryption capabilities.
SOAP	A standard lightweight messaging protocol intended for exchanging structured information using XML technologies. Cisco Jabber uses SOAP to connect to the CUCM Instant Messaging & Presence (IM&P) server and download its configuration.
XMPP	A communications protocol for message-oriented software based on XML.

Protocol	Description
LDAP	Provides a mechanism to connect to, search, and modify internetwork directories.
CTI	A technology allowing communication between a software application, such as Cisco Jabber, and a collaboration endpoint. Cisco Jabber uses CTI to control an associated desk phone.
CTIQBE	Allows an extension to CTI for Network Address Translation (NAT) / Port Address Translation (PAT), allowing telephony applications to function across a firewall.
CAST	Allows Cisco Jabber, in desk phone mode, to use separate hardware such as an attached webcam and a physical desk phone (non-video-capable) in a single communications instance. The video and audio are split and remain in sync throughout the call.
IMAP	A communications protocol for e-mail message retrieval and storage as an alternative to the Post Office Protocol (POP).

In terms of discussing call control protocols, it is important to distinguish between line-side and trunk-side protocols. As the names imply, these are protocols used in specific situations. Line-side protocols are used by call control elements to communicate with and process signaling requests to/from endpoints. Trunk-side protocols are similarly used in communicating with other call control entities. In terms of CUCM, there are two line-side protocols in use: SIP and SCCP. As mentioned in Table 4-2, SIP is an industry-standard protocol, and SCCP is a Cisco proprietary protocol. There is no real difference in the functionality or administration of a SIP phone versus an SCCP phone. The two protocols can coexist without issue in any Cisco collaboration solution.

Cisco IP Phone Configuration

Key Topic

For any endpoint to register with CUCM for call control or to run applications, it must be configured in advance. There are a few ways in which this can be accomplished:

- Auto-registration, which allows a phone to connect to the network and register to CUCM without any preconfiguration of that specific phone required.
- Manual configuration in advance of the phone connecting to the network (most common method).
- Through the use of the Cisco Prime Collaboration Provisioning (CPC) tool. CPC is beyond the scope for of this book and is not discussed further.

Regardless of the means used for configuration of endpoints, a number of basic settings/parameters on the phone must be taken into account, including the following:

- Media Access Control (MAC) address
- DHCP
- Static IP address
- TFTP server
- DNS

The MAC address is unique to the phone's network interface card (NIC). It needs to be recorded for entry into CUCM because this is the primary identifier for each endpoint. The method of IP address acquisition, whether through DHCP or static configuration, is not entirely relevant as long as it is properly done, one way or the other. DHCP is obviously the preferred method due to its dynamic nature. It does not require an administrator to physically configure each phone. The TFTP server acquisition can also be dynamic or static. It is typically included as Option 150 in the DHCP parameters for the voice/video VLAN. However, static configuration is often used even in environments where DHCP Option 150 is available. If a phone is to be moved to another cluster or needs to be part of a lab environment, the alternate TFTP option in the phone's configuration can be enabled and a static TFTP server or servers set. DNS is purely optional. It is most often used when the phone needs to reach applications and or destinations based on domain names rather than by IP address.

Auto-Registration

Key Topic

Auto-registration is certainly an option, but use of that feature should be carefully tempered with a touch of sanity. One does not simply allow any endpoint to connect to the network, register, and make calls without administrative oversight. Auto-registration is enabled or disabled in the CUCM administration interface under the **System > Cisco Unified CM Configuration** page. Select the Unified CM node that will play the role of primary call control node for auto-registering phones. Figure 6-1 shows a portion of the Cisco Unified CM Configuration page.

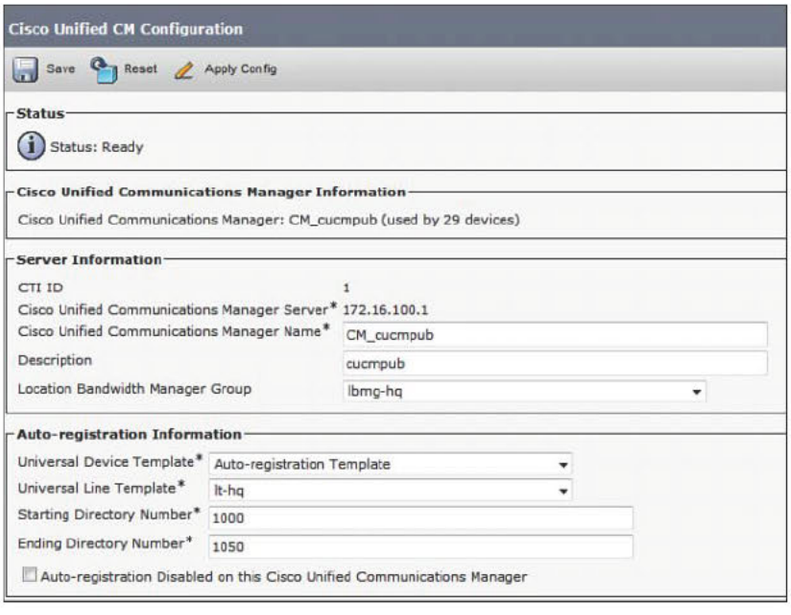


Figure 6-1 *Cisco Unified CM Configuration Page*

In the CM configuration options, select a universal device template and universal line template, which are preconfigured to a partition and calling search space that can call nowhere but to the self-provisioning pilot, assuming self-provisioning is enabled. Self-provisioning

is a relatively new feature that allows a user to add his/her own phone to the network with relatively little effort on the part of the administrator. A self-provisioning pilot number points to a CTI route point that launches a basic interactive voice response (IVR) script. The IVR asks for a self-provisioning identifier, which is predefined and user specific. Based on the user information, the phone is added to the system and associated with the user. Self-provisioning, like auto-registration, is dependent upon the configuration of universal device and line templates; otherwise, there is nothing to populate the required phone parameters for the user, such as directory number partition, calling search space, and others.

The configurations for both universal device template and universal line template are found in the CUCM administration under **User Management > User/Phone Add**. Figure 6-2 shows a cutout of the universal line template and the calling search space.

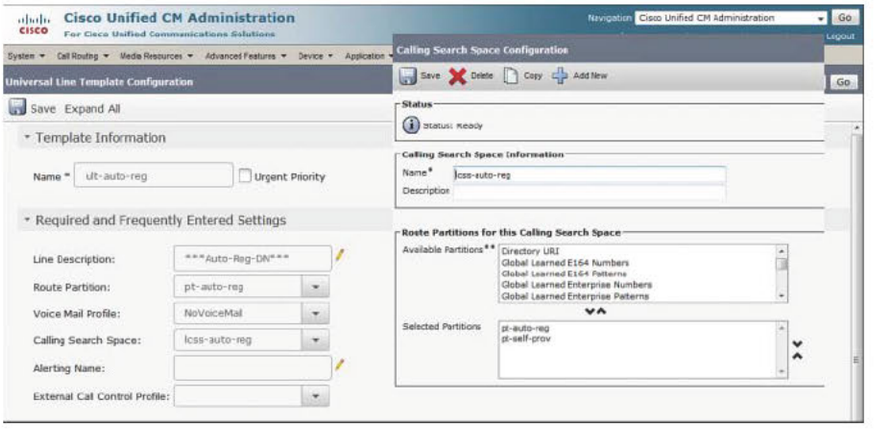


Figure 6-2 *Universal Line Template and Calling Search Space*

Auto-configuration is a simple way to enable a large number of phones to register to CUCM without fear of the dreaded fat-fingering of the phone's MAC address.

Manual Configuration

Key Topic

At first glance, it might seem that the Bulk Administration Tool (BAT) has been left out of the discussion. That is true, in part. The BAT does enable mass import of IP Phones, but not without considerable work ahead of time in building the comma-separated value (CSV) file needed for the import. With that in mind, the BAT is here, under the manual configuration. The BAT is beyond the scope of this discussion for the time being.

When manually configuring a collaboration endpoint, the first piece of information required is the endpoint type. In CUCM Administration, click **Device > Phone > Add New**. Clicking the **Add New** button displays a drop-down menu. Scroll to the appropriate endpoint type and select it. Once selected, there are two possibilities for what is presented next. If the device is capable of being provisioned as a SIP or SCCP endpoint, the line-side protocol must be selected, and then the configuration will proceed to the device configuration page. If the device is capable of only SIP, the device configuration page is presented.

On this page, you have numerous options. Only a few of them are actually required. The first of these is the MAC address. All the required fields have an asterisk next to the field names for emphasis. When you complete the device configuration and then click the **Save** button, a column of button configuration links is added vertically along the left side of the page according to the phone button template selected for the endpoint. Also, at this point, a configuration file for the phone is created and added to the TFTP server so that it can be downloaded once the phone connects. Using these newly provided links, directory number (DN) buttons, intercom buttons, busy lamp field (BLF) buttons, application buttons, and more can be assigned. Figure 6-3 shows a DX650 configuration page with an assigned DN.

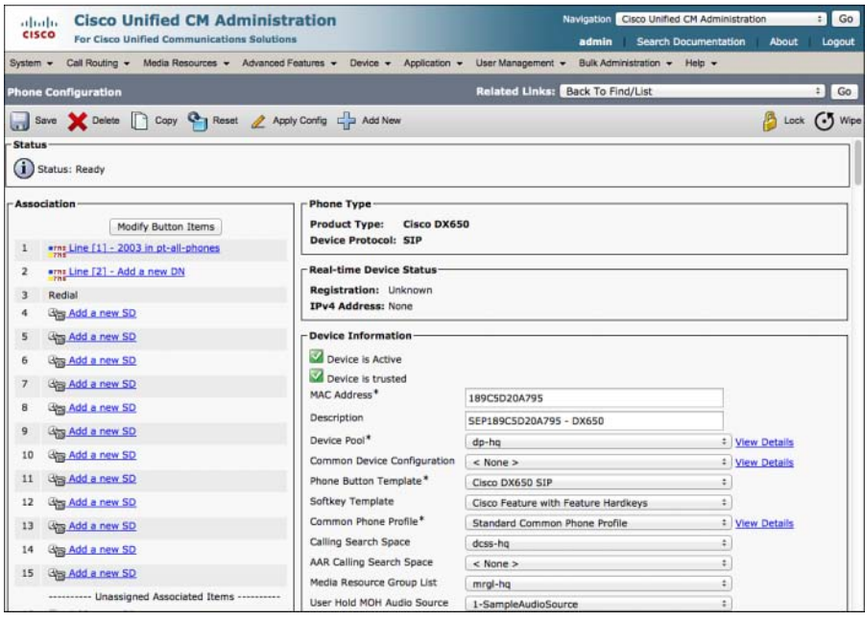


Figure 6-3 *Cisco DX650 Configuration Page*

In the figure, you can see the DN along with numerous configurable speed dial (SD) options. The device will register and download its firmware and configuration file once it is connected to the network and has booted completely.

One item of note in the new endpoints, 7800/8800, DX series, and so on is that the means by which firmware upgrades occur has been altered. In the past, when a phone registered, it downloaded its firmware immediately, before it was fully registered and usable. Now, firmware is downloaded while the device is in a usable state. The device will boot with its existing firmware, register, and be operational. When a firmware upgrade is needed, the firmware is downloaded in the background, and then the user is prompted to allow the end-point to reboot to complete the upgrade. This reduces the overall user impact of firmware upgrades/changes.

Note that when new phones are added to the portfolio, they have to be added to CUCM. This is done through the installation of a device pack. Device packs can be downloaded from the Cisco Communications Manager Updates page on Cisco.com. Individual phones

can be added manually; however, for purposes of maintaining the most up-to-date firmware for all endpoints, the device pack is preferred. Once the device pack is installed, there will be a full-cluster reboot required to complete the installation. So, be sure to schedule a maintenance window.

Should it become necessary to manually configure a phone, for some reason, all that is required is power. Whether that power comes from an actual power cord or via Power over Ethernet (PoE) is not overly important at this point. The settings for the endpoint are accessed by various means depending on the endpoint model. For the 7800/8800/9900 series phones, there is a button with an icon of a cog, which represents the settings. Figure 6-4 shows the 9971 and its settings button.

Figure 6-4 *Cisco 9971 Settings Button*

Upon pressing the settings button, a menu of options is shown on the screen. Select **Applications > Administrator Settings > Network Setup > Ethernet Setup**. On this screen, a number of options exist, including the ability to view the VLAN ID, domain name, or MAC address. In addition, the IPv4/IPv6 settings can be altered here. If the IP address needs to be statically configured, select IPv4 setup and ensure that the **DHCP Enabled** switch is set to **No**. (It is set to Yes by default.) At that point, the IP options can be manually entered. If a change is made, click **Apply**. More typically, there will be a need to specify an alternate TFTP server. Using the arrow keys, scroll down to the **Alternate TFTP** option and set it to **Yes**. Then enter the address of the TFTP servers as needed. Click **Apply**.

The 9971 is a video-capable phone, assuming it is ordered with the USB-attached camera. The camera connects to the back of the device and stands up to look over the back of the display. There are two primary concerns in enabling video on the device. The first is on the phone itself. Click the **Settings** button, and then choose **Applications > Accessories > Cisco Unified Camera Settings**. On this screen, set the **Auto Transmit Video** option slider to **On**. Select **View Area** to see a self-view and adjust the size of the viewable area which others will see during calls, and then click **Save**. The second part that needs to be checked is on the bottom of the 9971's device page in the CUCM Administration page. The options for the **Cisco Camera** and **Video Capabilities** need to be set to **Enabled**. Figure 6-5 shows the 9971 device configuration page with these settings enabled.

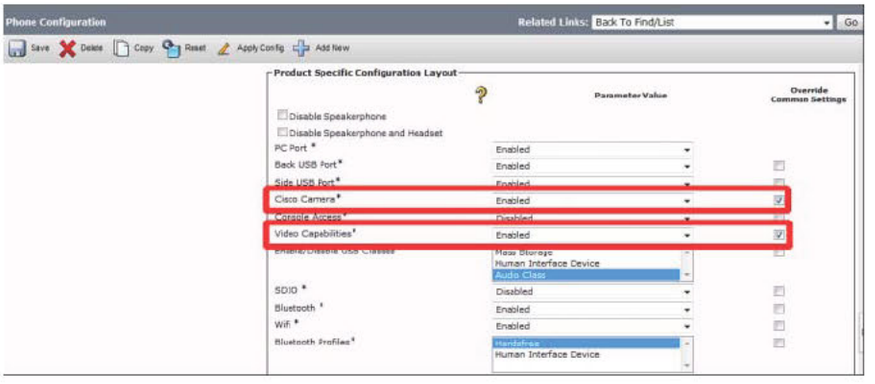


Figure 6-5 *Cisco 9971 Device Page*

You can configure these settings phone by phone or globally. The device page shown in the figure is the phone-by-phone method. There is a recently added page in CUCM Administration called Enterprise Phone Configuration. Open the CUCM Administration page, and click **System > Enterprise Phone Configuration** to set global phone parameters. When making changes on this page, also ensure that the **Override Common Settings** check box is checked. Otherwise, the setting will not update. The settings and parameters on this page are also configurable on the Common Phone Profile. So, that means that there are three distinct places within the CUCM Administration pages wherein some of these options may be altered. With that in mind, it is important to specify order of precedence (highest to lowest):

- Phone Configuration window settings
- Common Phone Profile window settings
- Enterprise Phone Configuration window settings

Cisco IP Phone Registration Process

Key Topic

The process through which endpoints progress to register with CUCM can seem a bit involved. However, it is a logical procedure that can be easily understood. Obviously, the first order of business is power. Power can be provided through the use of a power cube plugged into a wall outlet, or it can come from the LAN switch in the form of PoE.

Cisco created "inline power" in 2000 as a response to a growing desire in the IP telephony and wireless access arenas to be able to forego the need for power supplies on phones and access points, respectively. The idea of the phone drawing power from the wall jack to which it is connected is nothing new. At the time, there was no industry standard way of providing said power for IP Phones. When the IEEE ratified the 802.3af specification, Cisco retired the proprietary inline power functionality. The IEEE has further advanced the capabilities with the ratification of 802.3at PoE.

PoE is something of a science all on its own. There are a variety of levels of power that a LAN switch can provide. Usually, the level of PoE capabilities on the switch is based on its own power supply. In many cases, a switch's power supply may not be sufficient to allow for PoE to all ports. Or, it may only be able to provide a certain wattage per port. The wattage requirements for endpoints will certainly depend on the endpoint and its capabilities. Typically, the more feature-rich the endpoint, the more power required to run it. The industry refers to these power differences as the class of the device, ranging from Class 0 to Class 4. With regard to 802.3af, Classes 0–3 were used, and Class 4 was reserved. With 802.3at arriving on the scene, Class 4 has been defined, but only for 802.3at-capable devices. Table 6-3 shows the PoE classes and power specifications. There are two defined entities to keep in mind: power sourcing equipment (PSE) and powered device (PD). The PSE is the LAN switch, and the PD is the endpoint or access point.

Table 6-3 PoE Classes and Power Levels

Class	Wattage at PSE	Wattage at PD	Description
0	Up to 15.4W	0.44–12.94W	Default classification
1	Up to 4W	0.44–3.84W	Very low-power devices
2	Up to 7W	3.84–6.49W	Low-power devices
3	Up to 15.4W	6.49–12.95W	Mid-power devices
4	Up to 30W (802.3at)	12.95–25.50W	High-power devices

When the endpoint is connected to the access layer switch, if it is not connected to external power, it attempts to obtain power via PoE. Initially, the switch responds by going into what is called a resistive detection and classification stage. This is a protective mechanism to guard against damaging connected devices. There a resistance of 25 ohms in PoE-compliant devices. Assuming that stage passes, the switch responds by applying power in low power mode with 6.3W to allow the phone to boot. Cisco endpoints use CDP to make a specific request to Cisco switches for the amount of power they require. CDP also informs the endpoint of the voice/video VLAN ID to which it should attach. Optionally, LLDP-MED can be used for similar functionality.

With the phone now powered up sufficiently, the boot process continues. The next order of business is the acquisition of IP addressing and TFTP services. This is done via DHCP, assuming that static configuration is not being used. The endpoint broadcasts a DHCPDISCOVER on the VLAN provided by CDP/LLDP-MED. In response, one or more

DHCPOFFER messages is sent from the DHCP server to the requesting endpoint via unicast. The information in the DHCPOFFER includes the IP address, subnet mask, default gateway, DNS, and TFTP Option 150 address. With that information in hand, the endpoint can proceed on to the next step, contacting the TFTP server.

The TFTP Option 150 address contained in the DHCPOFFER is used to send a TFTP/HTTP GET request to the TFTP server. The request is looking for a specific filename based on the MAC address of the endpoint. The MAC address of the endpoint can be found on the back near the bottom, in most cases. Figure 6-6 shows the location of the MAC address on the back of an 8861 phone.

Figure 6-6 *Cisco 8861 IP Phone MAC Address Location*

Based on the endpoint model, the general layout will vary. At times, it will be in a row across the bottom of the device rather than as shown in the figure. Hopefully, the MAC address will have already been located as part of preconfiguring the phone in CUCM. However, if auto-registration was used, it may not have been manually located.

The file being requested at this point from the TFTP server is in the format SEP<*MAC ADDRESS*>.cnf.xml. So, if the MAC address were 00C0.1CBE.1EA8, the TFTP/HTTP GET request would be made for the file SEP00C01CBE1EA8.cnf.xml. Once the file is retrieved, it is parsed and loaded. The endpoint will also examine its running firmware version versus the version specified in the configuration file. If so, it continues on with the registration process. If not, it requests the firmware files.

Newer models, such as 7800/8800/DX series endpoints, continue to boot and register, regardless. They download the new firmware in the background without impacting phone operation. Once the files are loaded, the user gets a pop-up with a request to restart the phone. With earlier phone models, the registration process stalled while the new firmware files were downloaded and executed.

Once the firmware is in place, the phone sends a SIP REGISTER message to CUCM, assuming SIP is the line-side protocol configured for the phone. CUCM responds with a SIP 200 OK message, and the process is complete. With SIP, you have additional options to download and use local dial-plan information and dialing rules to each phone. The phone can also download additional ring tones, localization files, and other customizable functionality files. At this point, the registration is complete, and the endpoint should be in usable state. Figure 6-7 shows an overview of the process as discussed thus far.

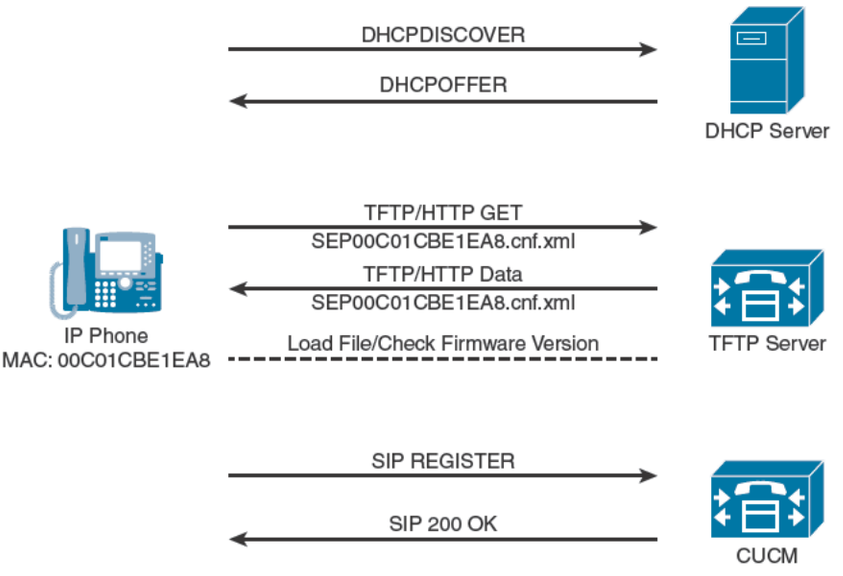


Figure 6-7 *Cisco Endpoint Registration Process Overview*

Cisco Jabber Configuration

Key Topic

Cisco Jabber is an all-in-one client for desktop and mobile devices. It is based on a Client Services Framework (CSF). The CSF aids in making the development cycle more agile across the various clients. It provides IM, presence, video, voice, calendar integration, e-mail integration, screen sharing, conversation escalation, and more. It relies on a number of protocols aside from those typically associated solely with telephony. It can be deployed in a number of modes as well. Table 6-4 lays out the modes for Jabber deployment.

Table 6-4 Cisco Jabber Deployment Modes

Mode	IM	Presence	Telephony	Video
IM only	Yes	Yes	No	No
Phone	No	No	Yes	Yes
Full UC	Yes	Yes	Yes	Yes

The underlying architecture involved with Cisco Jabber deployments varies depending on whether the IM portion is to be on-premises based or cloud based. In the cloud-based deployment, all services for call control, calendar integration, desk phone control, and so on are deployed within the local enterprise. However, the IM aspects of the Cisco Jabber client are based in the WebEx cloud as a hosted service. For on-premises deployments, all aspects are, as the name implies, on-premises. Figure 6-8 shows a typical Cisco Jabber deployment architecture.

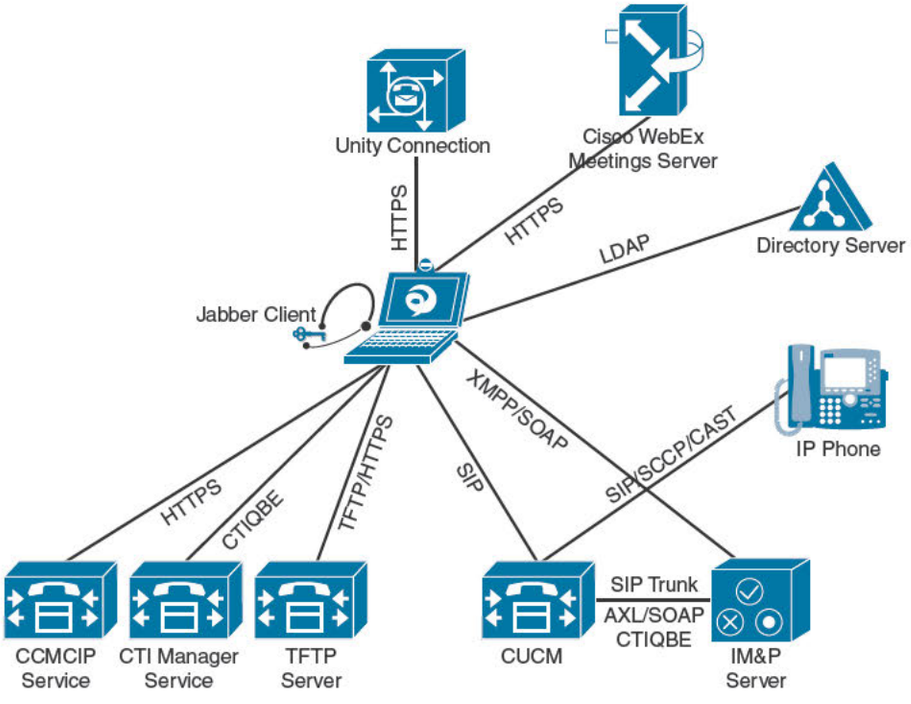


Figure 6-8 *Cisco Jabber Architecture*

The figure shows only those protocols and connections relevant to the Jabber client itself. Obviously, the picture is incomplete from the perspective of all of the other components shown therein. The Cisco UCM IM&P server, formerly known as Cisco Unified Presence Server (CUPS), is required to provide presence and IM capabilities to end user clients.

CUCM is required to provide call control as well as licensing and the user database for the IM&P server. In full UC mode, a single IM&P server can support up to 15,000 users. A cluster of three IM&P servers can support up to 45,000 users for full UC. High availability (HA) is also an option in the IM&P server architecture. For IM-only deployments, a single server can support 25,000 users and a cluster, 75,000 users. The HA option is available for this deployment as well. When configuring Jabber in CUCM (for full UC and phone mode), a CSF profile is required. This is the equivalent of an endpoint configuration for a physical endpoint. The device name in CUCM needs to begin with CSF, followed by an arbitrary identifier, usually a user ID. For example, CSFJDOE would be the device name for John Doe's Jabber device in CUCM.

Jabber users are identified by a Jabber ID (JID). It consists of a Jabber username and a domain name in much the same way an e-mail address or a URI is formatted. Users can be created on CUCM or synchronized from an Active Directory (AD) or LDAP server. User authentication is done by CUCM for locally created users and proxied to the AD/LDAP server for synchronized users.

Jabber makes use of SOAP over HTTPS upon its launch in communicating to the IM&P server to retrieve its configuration. Jabber makes contact with CUCM via HTTP and HTTPS to retrieve a list of devices associated to the user who is logging in. XMPP is used in communication with the IM&P Server for presence status and IM functionality. LDAP is used for directory searches when looking for contacts with whom to communicate.

From a telephony perspective, Jabber is a soft phone registering to CUCM. As such, it acts very much like the endpoints discussed earlier in this chapter. It makes contact with the TFTP server, pulls its configuration file, and then registers to CUCM as a SIP endpoint. It can use both RTP and SRTP for media in both audio and video communications as configured by the CUCM administrator.

Jabber makes use of a Cisco CallManager Cisco IP Phone (CCMCIP) service profile in retrieve settings and information about devices associated with a particular user. This list of devices is used in populating the Desk Phone Control field in the Jabber client.

In communicating with Unity Connection, the Jabber client uses an IMAP connection to retrieve and manage the list of voice messages for the logged-in user and to retrieve and manage the messages themselves.

Note While divided into component services in Figure 6-8, it is highly probable that the TFTP server, CTI Manager service, and CCMCIP service will all be running on CUCM. Certainly, they will be running on a CUCM node, if not the CUCM Publisher itself. They do not have to be on individual node instances.

Cisco Jabber Installation and Registration Process

Jabber can be run in soft phone mode, wherein it functions as a voice/video-capable endpoint entirely independent of other devices or associated phones. Alternatively, Jabber can run in desk phone mode. In this mode, the Jabber client is in constant contact with an associated desk phone and uses it according to its capabilities. If the phone is capable of audio only, Jabber looks for a locally attached webcam on the desktop client and makes use of it should it be available. If the desk phone is both audio and video capable, Jabber makes use of the audio and video resources on the desk phone. Figure 6-9 shows a side-by-side view of the selection of soft phone mode and desk phone mode on the Cisco Jabber for Mac client.

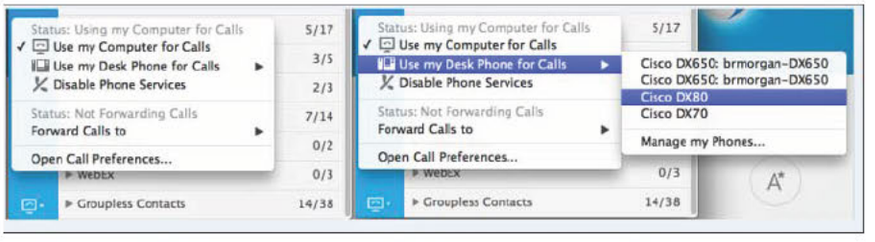


Figure 6-9 *Cisco Jabber for Mac Phone and Call-Forwarding Preferences Menu*

In the figure, the left side shows that the soft phone mode selection is made by clicking the **User my Computer for Calls** option. For desk phone mode, it is possible to expand the field to select from a list of associated phones to have Jabber use it for audio/video. The reason this is important is that the soft phone/desk phone selection determines how the Jabber client registers. If registering in soft phone mode, the Jabber device configured in CUCM will be used. If in desk phone mode, it will not. More on that shortly.

Service Discovery

Key Topic

To register and function fully, Jabber needs to know where its services are located and how to authenticate the user. This is accomplished through a process that includes both service discovery and a bootstrap or Universal Resource Locator (URL) configuration. It can also simply read predefined information in a configuration file downloaded from the CUCM TFTP server, called jabber-config.xml. Regardless of whether Jabber is launched from a desktop computer, smartphone, or tablet, it can automatically detect whether it is inside the network or outside the corporate network. It does this by detecting network change events, such as the switching of a smartphone from using its wireless network radio to using cellular data.

Jabber can be configured to prompt the end user to enter a user ID with the domain name, or the JID. Figure 6-10 shows the login prompt presented on Jabber for Windows.

Figure 6-10 *Cisco Jabber for Windows Login Prompt*

Jabber will use the domain portion of the JID provided to resolve the services via DNS SRV records. Optionally, an administrator can provide the domain name either via modifications to the Windows Installer or through a URL configured in the local jabber-config.xml file. In this case, the user will not need to provide domain information. Regardless of the method used, it then caches the domain information for future logins.

Jabber sends HTTP and DNS requests simultaneously in search of its services. This allows the discovery of on-premises and cloud-based services. The HTTP requests are sent to the Cisco WebEx Cloud service. The DNS requests are sent to the configured, either statically or dynamically, DNS servers for the client. When configuring the DNS SRV records, the fully qualified domain name (FQDN) of the respective entities to which the records refer should always be used. That, of course, also adds a requirement that DNS A records be created for each CUCM node, the IM&P server, and the VCE-E or Expressway-E as applicable. Table 6-5 shows the DNS SRV records used by Jabber for service discovery.

Table 6-5 Cisco Jabber DNS SRV Records

DNS SRV Record	DNS	Resolves To
_cisco-uds._tcp.domain.com	Internal	CUCM FQDN
_ cuplogin._tcp.domain.com	Internal	IM&P server FQDN
_collab-edge._tls.domain.com	External	VCS-E or Expressway-E FQDN

These SRVs will be configured in either internal or external DNS as noted in the table. Do not add the _cisco-uds or _cuplogin SRV entries to external DNS. If the client is inside the corporate network, DNS will return the internal network address of the services needed (in this case, _cisco-uds and _cuplogin). If the client is logging in from outside the corporate network, external DNS will return the external network address of the services (in this case, _collab-edge). There can be multiple entries for each of the SRVs with varying priorities/weights to provide for redundant connectivity. Example 6-1 shows an internal DNS configuration for the relevant SRVs with redundancy.

Key Topic

Example 6-1 *Jabber Internal DNS SRV Records*

```
Internal DNS Records

A Records:

sub01.domain.com 43200 A 172.16.100.2
sub02.domain.com 43200 A 172.16.100.3
pub.domain.com 43200 A 172.16.100.1

SRV Records:
_cisco-uds._tcp.domain.com
          Priority = 6
          Weight = 30
          Port = 8443
          svr hostname = sub01.domain.com
_cisco-uds._tcp.domain.com
          Priority = 2
          Weight = 20
          Port = 8443
          svr hostname = sub02.domain.com
_cisco-uds._tcp.domain.com
          Priority = 1
          Weight = 5
          Port = 8443
          svr hostname = pub.domain.com
_cuplogin._tcp.domain.com
          Priority = 8
          Weight = 50
          Port = 8443
          svr hostname = imp01.domain.com
_cuplogin._tcp.domain.com
          Priority = 5
          Weight = 100
          Port = 8443
          svr hostname = imp02.domain.com
_cuplogin._tcp.domain.com
          Priority = 7
          Weight = 4
          Port = 8443
          svr hostname = imp03.domain.com
```

Example 6-2 shows an external DNS configuration with redundancy records.

Key Topic

Example 6-2 *Jabber External DNS Records*

```
External DNS Records
A Records:

expwe01.domain.com 43200 A 1.1.1.1
expwe02.domain.com 43200 A 1.1.1.2
expwe03.domain.com 43200 A 1.1.1.3

SRV Records:

_collab-edge._tls.domain.com
          Priority = 3
          Weight = 7
          Port = 8443
          svr hostname = expwe01.domain.com
_collab-edge._tls.domain.com
          Priority = 4
          Weight = 8
          Port = 8443
          svr hostname = expwe02.domain.com
_collab-edge._tls.domain.com
          Priority = 5
          Weight = 0
          Port = 8443
          svr hostname = expwe03.domain.com
```

It is possible to configure the necessary settings manually, of course. Figure 6-11 shows the options in the Jabber for Windows client for manual configuration.

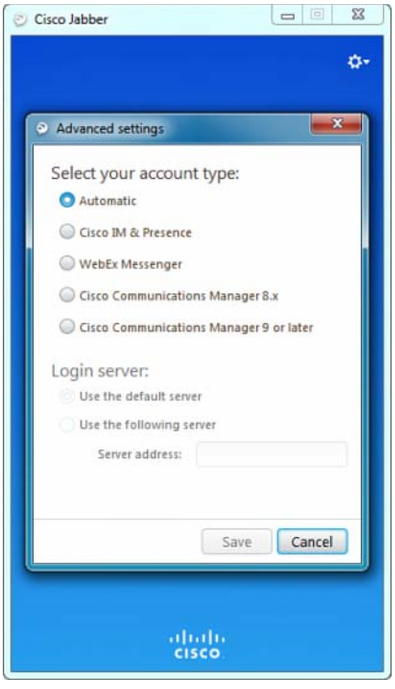


Figure 6-11 *Cisco Jabber for Windows Manual Configuration*

If configured manually, the client may not have the flexibility to roam into and out of the network as the addresses configured inside the network may be different than those required outside of the network. For this reason, the automatic configuration and service discovery using DNS SRV records is the preferred way to deploy.

When the client makes contact with the IM&P server, the determination as to whether the user is permitted to use Jabber is made. This validation is done by CUCM. A check box on the user page allows the use of IM and Presence. Figure 6-12 shows the End User Configuration page.

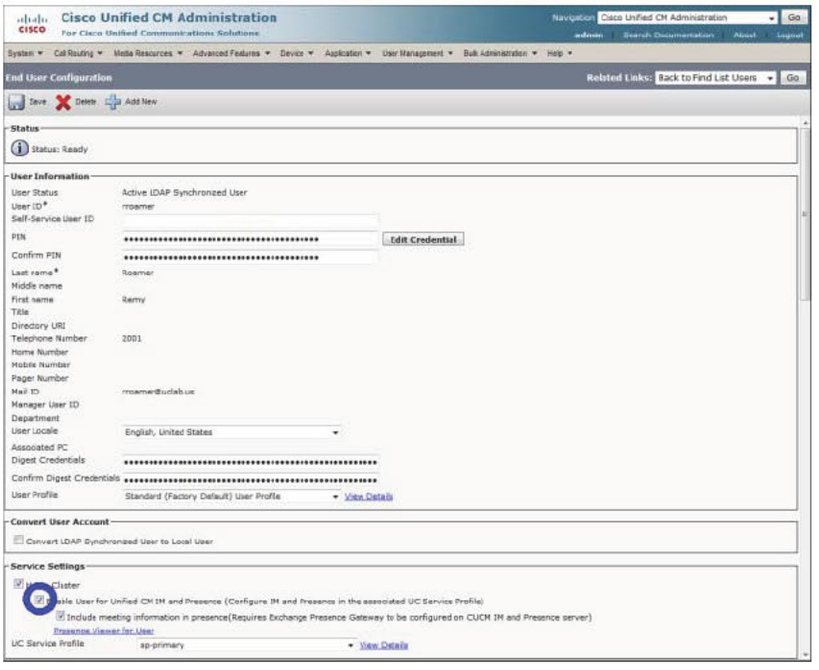


Figure 6-12 *Enable User for IM&P in CUCM End User Configuration Page*

Login and Registration

Key Topic

Assuming that the user is permitted to use IM&P, the IM&P passes the login information on to CUCM for authentication. Authentication is either processed locally on the CUCM database, if using User Directory Services (UDS), or forwarded on to the configured LDAP server, if LDAP integration has been implemented. With services discovered and login credentials validated, the user's contact list is downloaded via SOAP, and presence status of each of the configured contacts is updated via XMPP.

Within the CUCM configuration, UC Service Profiles have been created in support of Jabber clients. The client then requests a list of IP Phones associated with the user to populate the phone and call-forwarding selection menu (shown in Figure 6-9).

The UC Service Profile is a listing of each of the services relevant to the Jabber client, including the following:

- **Voice-Mail Profile:** Voice mail server that should be used
- **Mailstore Profile:** Mailstore server
- **Conferencing Profile:** Selection of available WebEx Cloud, CWMS, and so on
- **Directory Profile:** LDAP directory for contact search
- **IM and Presence Profile:** IM&P cluster with which to associate
- **CTI Profile:** Server used for CTI control
- **Videoconference Scheduling Portal Profile:** TMS instance for videoconference resource scheduling

If the user is logging in using soft phone mode, a TFTP request is made for the configuration file for the associated Jabber client device provisioned in CUCM. The formatting of the device name is dependent on the type of client logging in. Each of the options, however, should include the prefix and the username. For example, user1@domain.com would have an associated Jabber for Windows device named CSFUSER1 in CUCM. The Jabber client then issues a SIP REGISTER message to CUCM, which then responds with SIP 200 OK. The Jabber client can now make calls. In addition to registering with CUCM, the Jabber client will log in to the other configured services in the UC Service Profile (for example Unity Connection). When it contacts Unity Connection, it pulls a list of messages and the read/unread state of each.

If the Jabber client is logging in using desk phone mode, it initiates a CTI connection to the CUCM CTI Manager for desk phone control. It can then control the on-hook/off-hook state of the phone and its available resources for audio/video.

Tuning

The Jabber client can be tuned for audio and video operating levels at both the operating system (OS) level and within the Jabber client. A camera must be connected to the desktop machine for the Jabber client to use local video. In like fashion, there must be an existing microphone and speakers for audio to function properly in soft phone mode. Figure 6-13 shows the tuning options in the Jabber for Mac preferences configuration.

Figure 6-13 *Jabber for Mac Tuning Preferences*

The Audio/Video tab in the preferences settings of the Jabber client allows the selection of video source, in addition to audio input and output selection and microphone sensitivity and volume adjustment.

Cisco Collaboration Endpoint Status Verification

Key Topic

Although each collaboration endpoint model might look and function somewhat differently than others, they can all report on their current status, call statistics, network information, and so on. With any endpoint, the first bit of status is available when it is connected to power. During the boot process, the endpoint displays various messages depending on where it is within the boot process. A 9971 IP Phone will light the light-emitting diodes (LEDs) on its buttons as a progress indicator of boot progress, first amber and then green. Then it will show "Phone Not Registered" at the top of the screen while it retrieves its IP address and TFTP server information. Once the phone makes contact with the TFTP server, it pulls its configuration file, checks its firmware, and displays "Registering." When it makes contact with the primary call control node in its configuration, it displays the configure buttons and line text labels. At that point, the phone is registered and ready to make calls.

The Cisco 9971 has a number of additional informational aspects built in for the purpose of providing status about its software version, its connectivity to CUCM, its current status, and more. Figure 6-14 shows the Phone Information screen for the 9971 phone.

Figure 6-14 *Cisco 9971 Phone Information Screen*

The screen shown in the figure is accessed by pressing the **Applications** button (represented by the silhouette of a cog), then **Phone Information**. Information provided on this screen includes the phone's model number, IP address, hostname (a.k.a. device name in CUCM), firmware version, when it last upgraded that firmware, and the active CUCM call control node.

There is a specific menu within the Administrator Settings for Status information. The submenus provide a significant amount of information about the phone, its connectivity, both wired and wireless. This discussion covers only the wired information. It also includes information about call quality. The options here include the following:

- Status Messages
- Ethernet Statistics
- Wireless Statistics
- Call Statistics
- Current Access Point
- Wireless Site Survey

The Status Messages screen contains event log information such as TFTP file download verification, TFTP file timeouts, trust list updates, virtual private network (VPN) connection information, and so on. If the phone is not registering for some reason, clues to the reasons why that is the case may often be found here. Figure 6-15 shows the status screen of the 9971.

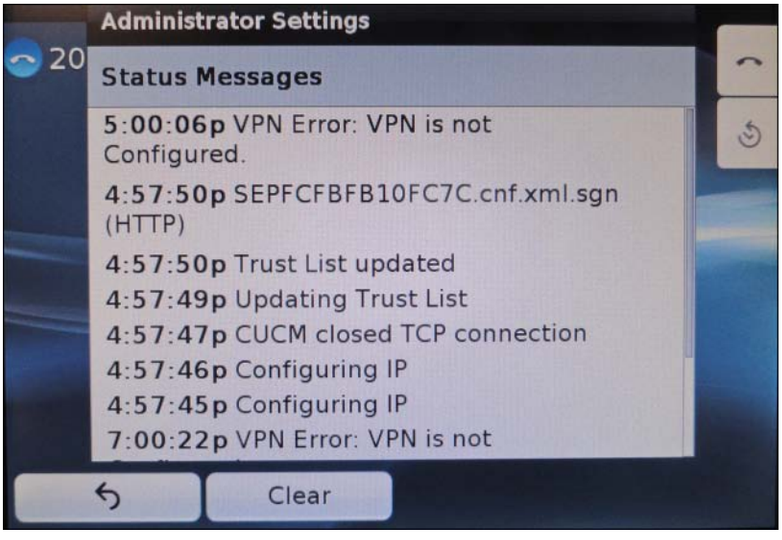


Figure 6-15 *Cisco 9971 Phone Call Statistics Screen*

Network connectivity options on the 9971 include both wired and wireless options. When connected to the wired interface, the Ethernet Statistics screen shows receive and transmit frames, broadcasts, connection time, and speed/duplex information. The Wireless Statistics screen provides much of the same information, though it adds multicast and QoS-related information.

Figure 6-16 shows the 9971 Ethernet Statistics screen.

Figure 6-16 *Cisco 9971 Phone Ethernet Statistics Screen*

While a call is in progress, there is a status screen for call statistics. It can be accessed through the Application menu. Once there, touch **Administrator Settings > Status > Call Statistics**. Figure 6-17 shows the Call Statistics screen.

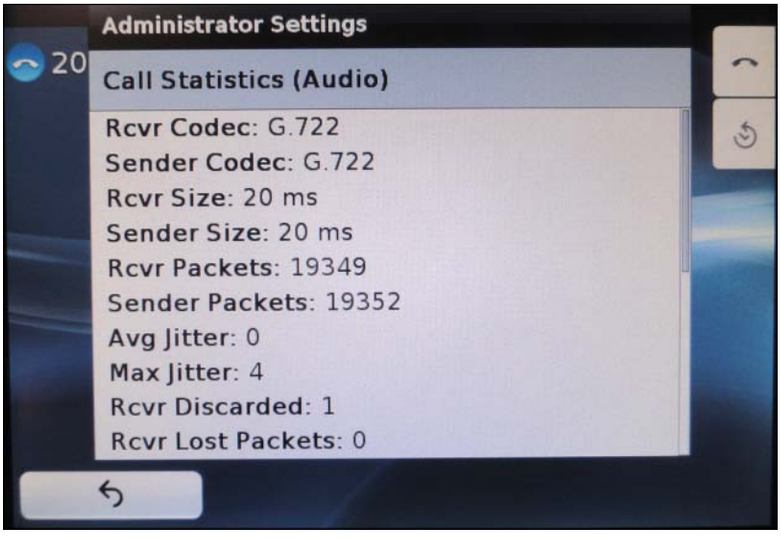


Figure 6-17 *Cisco 9971 Phone Call Statistics Screen*

In the figure, information relevant to the call in progress is shown. This includes codec selection and payload size. It also provides a count of packets sent and received and information about jitter and dropped packets. This screen is somewhat useful for troubleshooting issues such as codec mismatches and one-way audio problems.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 6-6 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 6-6 Key Topics for Chapter 6

Key Topic Element	Description	Page Number
Table 6-2	Describes protocols used by Cisco collaboration endpoints	131
Section	Explains the essential requirements for configuration of Cisco IP Phones in CUCM	132
Section	Describes how to enable and use auto-registration for Cisco IP Phones	133
Section	Describes how to manually configure Cisco IP Phone required parameters in CUCM and on the phone itself	134
Section	Explains the basics of PoE and how Cisco IP Phones obtain their configuration files and firmware to boot and register successfully to CUCM	137
Section	Describes the modes of operation for Cisco Jabber along with the architecture and scalability capabilities of Cisco UCM IM&P server	140
Section	Explains how Jabber finds the services it requires whether inside or outside the network	143
Example 6-1	Details the configuration of the required DNS A and SRV records in Internal DNS for Jabber functionality	145
Example 6-2	Details the configuration of the required DNS A and SRV records in External DNS for Jabber functionality	146
Section	Describes the Login process used by Jabber and how it accesses services offered within the Cisco collaboration architecture	148
Section	Describes the real-time feedback and status messaging mechanisms available in Cisco collaboration endpoints	150

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

802.3af PoE, 802.3at PoE, active load, Active Directory (AD), auto-registration, Bulk Administration Tool (BAT), busy lamp field (BLF), calling search Space, Cisco Audio Session Tunnel (CAST), Cisco CallManager CCMCIP, Cisco Discovery Protocol (CDP), Cisco Prime Collaboration, Class 0 PoE, Class 1 PoE, Class 2 PoE, Class 3 PoE, Class 4 PoE, Computer Telephony Integration (CTI), Computer Telephony Interface (CTI) route point, Computer Telephony Interface Quick Buffer Encoding (CTIQBE), Cisco Unified Communications Manager (CUCM), Dynamic Host Configuration Protocol (DHCP), DHCPDISCOVER, DHCPOFFER, directory number (DN), Domain Name Service (DNS), DNS A record, DNS SRV record, external DNS, Expressway-C, Expressway-E, firmware, Fully Qualified Domain Name (FQDN), GET, Hypertext Transfer Protocol (HTTP), Institute of Electrical and Electronics Engineers (IEEE), Instant Messaging & Presence (IM&P), Internet Message Access Protocol (IMAP), inactive load, inline power, internal DNS, Jabber full UC, Jabber IM&P, Jabber Phone, Jabber ID (JID), Lightweight Directory Access Protocol (LDAP), light-emitting diode (LED), Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED), Media Access Control (MAC) address, Option 150, partition, Real-time Transport Protocol (RTP), Skinny Call Control Protocol (SCCP), Session Initiation Protocol (SIP), SIP 200 OK, SIP REGISTER, Simple Object Access Protocol (SOAP), Secure Real-time Transport Protocol (SRTP), Transmission Control Protocol (TCP), Transmission Control Protocol/Internet Protocol (TCP/IP), Trivial File Transfer Protocol (TFTP), User Datagram Protocol (UDP), User Data Services (UDS), universal device template (UDT), universal line template (ULT), Universal Resource Locator (URL), Video Communications Server (VCS) control, Video Communications Server (VCS) Expressway, Extensible Messaging and Presence Protocol (XMPP)

This page intentionally left blank

This chapter covers the following topics:

- **Cisco TelePresence Endpoint Portfolio Overview:** This section describes the entire Cisco TelePresence Endpoint portfolio.
- **Cisco TelePresence CTS Software-Based Endpoint Characteristics:** This section describes characteristics of the CTS endpoints, which include the CTS 500-32, TX1300-65, and the TX9000. This section also introduces the new IX5000.
- **Cisco DX Series Endpoint Characteristics:** This section describes the characteristics of the Cisco DX endpoints, which include the DX650, DX70, and DX80.
- **Cisco TelePresence TC Software-Based Endpoint Characteristics:** This section describes the characteristics of the Cisco TC endpoints, which include the SX10, SX20, SX80, MX200G2, MX300G2, MX700, MX800, C40, C60, C90, and Cisco TelePresence System Profile Series.
- **Cisco TelePresence TC Software-Based Endpoint Peripherals:** This section discusses the peripheral components that can be added to any TC software-based endpoint.
- **Cisco Intelligent Proximity for Content Sharing:** This section discusses this new technology Cisco created that enables users to interface with their video endpoints from smartphones, tablets, and computers.
- **Cisco Jabber Video for TelePresence Characteristics and Installation:** This section describes characteristics of Jabber Video for TelePresence, what components are needed for it to work, and how to configure them.

CHAPTER 7

Cisco TelePresence Endpoint Characteristics

Much of the growth Cisco has experienced throughout the years has been attributed to key acquisitions. In doing so, Cisco has developed a vast range of product offerings for customers to choose from. In addition, Cisco differentiates between Unified Communications (UC) endpoints and TelePresence endpoints. And if that is not confusing enough, there are significant differences between Cisco TelePresence endpoints as well.

This chapter discusses TelePresence endpoints within Cisco's product line. This chapter notes key differences between the software bases for each product grouping, identifies what call control servers can be used for each product grouping, and discusses relative characteristics for each endpoint.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 7-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 7-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco TelePresence CTS Software-Based Endpoint Characteristics	1–2
Cisco DX Series Endpoint Characteristics	3
Cisco TelePresence TC Software-Based Endpoint Characteristics	4–7
Cisco TelePresence TC Software-Based Endpoint Peripherals	8
Cisco Intelligent Proximity for Content Sharing	9
Cisco Jabber Video for TelePresence Characteristics and Installation	10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What technology does TIP use during immersive calls that allows endpoints to conserve bandwidth and streamline the sending and receiving of audio and video?

   a. Real-time Transport Protocol
   b. Multiplexed media
   c. User Datagram Protocol
   d. Replication

2. Which CTS software-based endpoint is an ideal solution for an executive office?

   a. DX80
   b. EX90
   c. CTS 1100
   d. CTS 500

3. What is the software base for the DX series endpoints?

   a. TC
   b. Android
   c. Apple IOS
   d. CTS

4. Which Integrator solution uses EuroBlocks for audio connections?

   a. SX20
   b. SX80
   c. C60
   d. C90

5. How many XLR mic outputs does the C90 have?

   a. 2
   b. 4
   c. 6
   d. 8

6. Which of the following features differentiates the MX300 G2 endpoint from the MX300 endpoint?

   a. 55-inch monitor
   b. 1920x1200 resolution
   c. 1 PC port
   d. 2-2nd input sources

7. Which of the following is not a feature that comes with the MX800 endpoint?

   a. 1-70 inch monitor
   b. 2-55 inch monitors
   c. **3+1** multipoint call support at 1080p30
   d. 4+1 multipoint call support at 720p30

8. Which of the following cameras is supported with the SpeakerTrack dual camera option?

   a. Cisco Precision HD 1080p camera with 4x zoom
   b. Cisco Precision HD 1080p camera with 12x zoom
   c. Cisco Precision 60 1080p camera with 20x zoom
   d. Cisco precision HD 1080p USB camera

9. What technology does Cisco use with Intelligent Proximity for Content Sharing that allows computers, smartphones, and tablets to connect with endpoints?

   a. Bluetooth
   b. High-frequency sound waves
   c. IP WLAN to LAN connection
   d. Circuit-switched connection

10. Which of the following is not a component used when deploying a Jabber Video for TelePresence solution?

    a. Cisco VCS
    b. Cisco TMS
    c. Cisco Unified CM
    d. DNS

Foundation Topics

Cisco TelePresence endpoints can be grouped into three main categories: Cisco TelePresence System (CTS), desk endpoints (DX), and TC. Each of these categories is based on the software kernel that drives the endpoint. Cisco engineers developed the CTS endpoints and the DX endpoints in-house. The TC endpoints were originally part of an acquisition, though Cisco has taken that seed and cultivated a premium product line that surpasses all others in the industry. This chapter provides an overview of each of these products.

CTS Software-Based Endpoint Overview

When Cisco was first expanding their UC products into the TelePresence arena, they developed the CTS firmware. Based on Red Hat, this firmware is similar to the underlining firmware used with the Cisco Unified Communications Manager (CM). The first CTS endpoint Cisco came out with was an immersive telepresence room solution known as the CTS 3000. This high-functioning six-person solution used three endpoints, a camera cluster of three cameras, three 65-inch primary monitors for displaying incoming video, and a fourth 42-inch monitor for displaying incoming content being shared. The lighting and all peripheral devices used where designed to offer a premium quality experience to the call participants. It was so great that while in use the technology would melt away, and you would feel like you were sitting in the same room as the participants on the other side of the call. To fully understand a protocol Cisco created to enable this system to function proficiently, you must first understand what ports a single-screen system uses in a call. Note that a single-screen system refers to a node that uses only a single endpoint, though dual monitors could still be used.

In a point-to-point video IP call between two single endpoints, a minimum of eight User Datagram Protocol (UDP) ports must be opened for the call to take place. Two audio and two video ports need to be open in each direction to carry the Real-time Transport Protocol (RTP) and RTC Control Protocol (RTCP) data. RTP is used to carry all the actual media, and RTCP is used to carry the signaling. Additional ports may need to be opened for other functions of an endpoint, such as far-end camera control and content sharing. Figure 7-1 illustrates the media and signaling ports that need to be opened for this type of call.

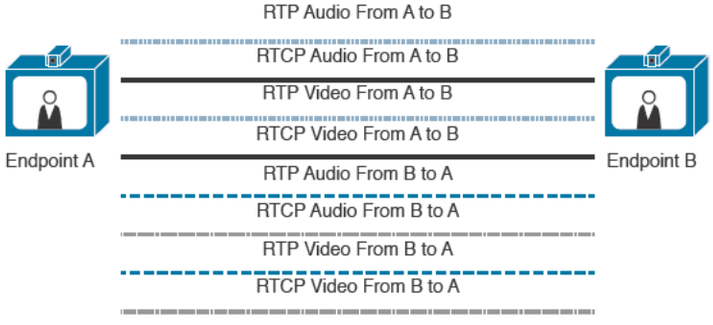


Figure 7-1 *Media and Signaling Ports*

Key Topic

The CTS 3000 system incorporates three endpoints in a single call. Therefore, 24 ports minimum would need to be opened for a two-way communication between two of these systems. To operate in a more efficient manner, Cisco developed a proprietary protocol that multiplexed the RTP and RTCP media and signaling traffic into a single RTP and RTCP stream. The way this works is the left and right endpoints send their traffic to the center endpoint, which is designated as the master. The master endpoint combines its own traffic, along with the left and right endpoints' traffic, and multiplexes the media together before sending it to the destination. When the destination endpoint receives this multiplexed media, the center endpoint demultiplexes it and distributes the information to the appropriate monitors and speakers. The destination sends traffic in the other direction by the same manner. Figure 7-2 illustrates how the multiplexing media process works.

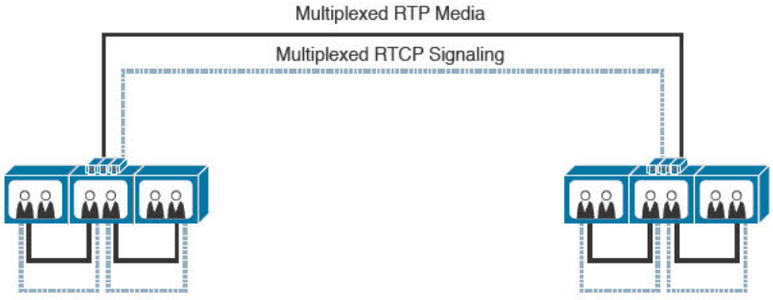


Figure 7-2 *Multiplex Media Process*

When Cisco purchased TANDBERG, they made this multiplexing process available as an open protocol and named it TIP, TelePresence Interoperability Protocol. TIP is available today for any company to use, and is managed by the International Multimedia Telecommunications Consortium (IMTC).

TANDBERG also had an immersive telepresence endpoint called the T3. Rather than offer two very different telepresence systems that would compete with each other, Cisco used technology from both products to develop a new immersive telepresence endpoint called the TX9000, and this immersive room system is based on the CTS firmware. After this solution was launched, Cisco made the CTS 3000 and the T3 end of sale. One of the many significant differences between the TX9000, CTS 3000, and T3 is that the TX9000 uses four codec endpoints rather than three.

The TX9000 is a great product but does have one limiting factor. A new codec was created for video feed that supports a higher pixilation saturation offering a better picture. It can also code and decode data in a more proficient manner, allowing for high-definition calls at a great reduction in bandwidth. This codec is known as H.265. Because of these major changes in capability, H.265 is hardware intensive, and endpoints need more than a software upgrade to support it. Therefore, the TX9000 cannot support H.265.

To incorporate this new technology into some of the endpoints available in a Cisco solution, Cisco developed a new endpoint that can support H.265 called the IX5000, which has been made available on the market since January 2015. The IX5000 has three screens like the TX9000, but uses a single endpoint with a separate codec box, rather than three to four

different codec endpoints. This flexible immersive telepresence solution can be used in any space the consumer desires to place it, without any specific room specifications, which is another quality the IX5000 has over any immersive telepresence solution on the market to date.

Key Topic

Some other CTS systems Cisco came out with are nonimmersive, but offer an excellent user experience. The CTS 500 is considered a personal TelePresence endpoint for a single user. Its intended use is for C-level employees to use in their office. The CTS 1100 and the CTS1300 were created as small conference room solutions. The CTS 1100 was intended for two participants, and the CTS 1300 was intended for up to six participants. Both products are now end of sale, and the CTS 1300 was replaced by the TX 1300. The TX 1300 still runs the CTS firmware.

All CTS software-based endpoints can register to the Cisco Unified CM only. Table 7-2 illustrates all the current endpoints Cisco offers in the CTS firmware platform with their capabilities.

Table 7-2 CTS Endpoint Capabilities

Endpoint Name	Purpose	Number of Participants	Platform Options	Mounting Options
CTS 500	Personal office system	1	1 32-inch monitor 1 manual camera	Pedestal Tabletop Wall mount
CTS 1100	Multipurpose room system	2	1 65-inch monitor 1 manual camera	Wall mount
TX1300	Multipurpose room system	6	1 65-inch monitor 3 manual cameras in cluster	Wall mount
TX9000	Immersive system	6 to 18	3 65-inch monitors 1 42-inch monitor 3 manual cameras in cluster	Purpose-built room
IX5000	Immersive system	6 to 18	3 70-inch monitors 3 auto cameras in cluster	Any-room system

DX Endpoint Overview

For a short time, Cisco had a video endpoint called the *Cius*. This endpoint was based on an Android OS and looked like a Cisco UC videophone, but the screen could be detached from the docking station, thereby making it a mobile video communications device. Unfortunately, at the time Cisco came out with this product, there were many soft clients that came out for tablets and mobile phones, making it not very marketable. Returning to the drawing board, Cisco came out with other Android-based endpoints called the DX series. These are fixed desktop solution endpoints that offer an incredible user experience.

The first and smallest of the DX endpoints is the DX650. Similar in design to the Cius, the DX650 is a phone that sits on the desktop, complete with a handset. There is a 7-inch touchscreen with a built-in camera that offers incredible HD video up to 1080p30 capability. The software for this DX endpoint is based on the Jellybean Android kernel. Though the monitor is small, it can be used as a second monitor for your computer and supports sharing content while in a video call using Binary Floor Control Protocol (BFCP). This is the only phone in the DX series that supports 802.3af PoE (Power over Ethernet), but a power cube can be used as well.

Cisco recently added two more endpoints to the DX product line. The DX70 has a 14-inch touchscreen display and supports the same android features as the DX650. Similar to design and function, the DX 80 sports a 23-inch touchscreen. Both these systems require a power cube, but because they use a touchscreen, neither needs an external remote control or other control device. All DX series endpoints register to the Cisco Unified CM only. Table 7-3 illustrates the different endpoints in the DX Series with their capabilities.

Key Topic

Table 7-3 DX Series Endpoint Capabilities

Endpoint Name	Display	Front Camera	Operating System	Processor	Storage
DX650	7-inch backlit, Widescreen Super Video Graphics Array (WSVGA) capacitive touchscreen liquid crystal display (LCD) with 1024x600 pixel resolution	High-definition video	Android 4.1.1	TI OMAP 4470 1.5 GHz	1 GB RAM
DX70	14-inch backlit, full high definition (FHD) capacitive touchscreen LCD with 1920x1080 pixel resolution	High-definition video	Android 4.1.1	TI OMAP 4470 1.5 GHz	2 GB RAM
DX80	23-inch backlit, FDH capacitive touchscreen LCD with 1920x1080 pixel resolution	High-definition video	Android 4.1.1	TI OMAP 4470 1.5 GHz	2 GB RAM

TC Software-Based Endpoint Overview

The TC software-based firmware came from the key acquisition of TANDBERG made in 2010, propelling Cisco into the telepresence market as the industry leader. Taking an already great product, Cisco has continued to build on this advantage and improve the quality of endpoints produced. All but one of the TC software-based endpoints can register to the Cisco Unified CM via Session Initiation Protocol (SIP) or to the Video Communications Server (VCS) via SIP/H.323. Cisco has divided these endpoints into categories based upon their primary intended purpose. The categories are SX, EX, and MX.

SX endpoints are solutions endpoints designed to integrate seamlessly into varying environments. The SX 10 is a unique endpoint because it is the only one that supports SIP only. Though limited in some of its functionality, this small endpoint offers full HD 1080P30 capability at a low cost. It can be purposed as a personal or small conference room solution. It comes with a TRC6 remote control and the all-in-one endpoint/camera. Another unique feature that sets this TC endpoint apart from the rest is that power can be supplied over PoE 802.3af. The SX 20 Quickset is a full-featured integrator endpoint for small to medium-sized conference rooms. As with all integrator endpoints, the SX20 comes with a camera, microphone TRC5 remote control, and all the cables and linkage for a basic setup. The pinnacle product of the SX endpoints is the SX80. This high-powered integrator endpoint was the first endpoint industry wide to support H.265. It also allows for use of EuroBlock connectors (also referred to as a Phoenix connector) so that integrators can run raw audio cables the exact lengths needed. Table 7-4 illustrates all the current SX endpoints with their capabilities.

Key Topic

Table 7-4 Current SX Endpoint Capabilities

Endpoint Name	Multisite	Audio Inputs	Audio Outputs	Video Inputs	Video Outputs
SX10	No	1 HDMI 1 minijack mic input 1 built-in mic	1 4-pin minijack 1 HDMI	1 HDMI 1 VGA	1 HDMI
SX20	576p 1+3	2 minijack mic input 1 minijack line in	1 minijack line out	1 HDMI 1 DVI-I	2 HDMI
SX80	1+4 at 720p30 1+3 at 1080p30	8 Microphones EuroBlock connector 4 Line-level EuroBlock 3 HDMI in (minijack)	6 line-level EuroBlock connector 2 HDMI	3 HDMI 1 DVI-I 1 BNC connector	2 HDMI 1 DVI-I

Though they are not SX endpoints, the C series endpoints are the pioneers of the TC software-based platform. There are three C series products that originated with TANDBERG: the C90, C60, and C40. The C90 is a two-rack unit (2RU) endpoint that has multiple different audio and video connectors. Supporting so many connection types offers integrators many options for peripheral connection in conference rooms. The C60 is a 1RU endpoint with half the connections available to the C90. However, this endpoint has the same internal capability as the C90 but offers a lower-cost integrator solution without compromising functionality. If functionality is not so much an issue, the C40 is a 1RU endpoint with half the connections as the C60, and a lot of the internal capability has been removed.

When integrators set up an A/V system in a room, often many different peripheral devices need to be added for improved functionality and performance. The C90 and C60 have many of these functions built in to them, so extra components are no longer needed. The

tools they possess include a video matrix switcher, digital audio mixer, video scalar, image compositor, and HD videoconferencing codec. The video matrix switcher is used for connecting multiple input and output devices like daisy-chaining cameras or connecting multiple display monitors. A C90 allows for up to seven cameras to be added in a daisy chain without any other peripheral device. The C60 allows for up to four cameras to be added in a daisy chain. The digital audio mixer combines or mixes and routes an audio signal. It also changes the level, timber, and dynamics of an audio signal. The video scalar converts an image that comes in at one resolution to another resolution if needed. The image compositor transcodes video coming in from different sources into a single image. The HD videoconferencing codec is used in multipoint calls, allowing these endpoints to host multipoint calls with three other endpoints using HD. The C90 supports multipoint calls up to 1080p30. The C60 supports multipoint calls up to 720p30. The C40 does not have these five extra functions built in to it. In a point-to-point call, the C40 can still support 1080p30, but in a multipoint call, it can only host calls at 576p30. Also, HD cameras cannot be daisy chained on a C40 without an external video matrix switcher. Table 7-5 illustrates all the current C-series endpoints with their capabilities.

Key Topic

Table 7-5 Current C Series Endpoint Capabilities

Endpoint Name	Multisite	Audio Inputs	Audio Outputs	Video Inputs	Video Outputs
C40	576p 1+3	2 XLR 2 RCA/phono 1 HDMI	2 RCA/phono 1 HDMI	2 HDMI 1 DVI-I 1 Composite	1 HDMI 1 DVI-I
C60	720p 1+3	4 XLR 2 RCA/phono 1 HDMI	2 RCA/phono 1 HDMI	2 HDMI 2 DVI-I 1 Composite	1 HDMI 1 DVI-I 1 Composite
C90	1080p 1+3	8 XLR 4 RCA/phono 2 HDMI	2 XLR 4 RCA/phono 2 HDMI	4 HDMI 4 HD-SDI 2 DVI-I 2 YPbPr 1 S-video 1 Composite	2 HDMI 2 DVI-I 1 Composite

Like the CTS 500, the EX endpoints offer a desktop solution intended for C-level executives. There are two EX endpoints available, and they both ship with Touch 8 controller. Also, the HD camera can be used as a document camera for sharing content simply by pointing it straight down. The EX60 has a 21.5-inch monitor and does not support the multisite option key. The EX90 has a 24-inch monitor and does support the multisite option key. Table 7-6 illustrates all the current EX endpoints with their capabilities.

Key Topic

Table 7-6 Current EX Endpoint Capabilities

Endpoint Name	Screen Size/ Resolution	Multisite	DVI and HDMI Inputs	HDMI Outputs	Integrated Audio
EX60	21.5 inch 1920x1080	No	1 (PC) 0 (second source)	None	1 integrated microphone 2 integrated front speakers
EX90	24 inch 1920x1200	1080p 1+3	1 (PC) 1 (second source)	Dual display option, audio input and output	1 integrated microphone 2 integrated front speakers and subwoofer

The MX endpoints are easy-to-deploy multipurpose room solutions that include all the components needed for use. The MX endpoints originated with the MX200 and MX300. These are all-in-one monitor/endpoint combinations that require only an Ethernet and power cable to operate. They come with a TRC5 remote control and can be integrated with the Touch 8 controller. The MX200 has a 42-inch monitor, and the MX300 has a 55-inch display monitor. However, these two endpoints do not support the multisite option. Cisco wanted to redesign these products and extend their functionality, so they came out with the MX200G2 and MX300G2 (G2 is for Generation 2). Though the screen size is the same, these two newer generation endpoints have a cleaner look, support the multisite option key, and come standard with a Touch 10 controller. Table 7-7 compares the MX200 and MX300 with the G2 models.

Key Topic

Table 7-7 Current MX200 and MX 300 Endpoint Capabilities

Endpoint	Video Quality	Screen Size / Resolution / Contrast Ratio	DVI and HDMI Inputs	HDMI Outputs	Multisite Options
MX200	1080p30/720p60	42 inch 1920x1080 2500:1	1 (PC) 0 (second source)	0	No
MX200G2	1080p60/720p60	42 inch 1920x1080 1300:1	1 (PC) 2 (second source)	1	1+4 at 720p30 1+3 at 1080p30
MX300	1080p30/720p60	55 inch 1920x1200 5000:1	1 (PC) 0 (second source)	0	No
MX300G2	1080p60/720p60	55 inch 1920x1200 4000:1	1 (PC) 2 (second source)	1	1+4 at 720p30 1+3 at 1080p30

The next MX endpoint is the MX700. This endpoint uses the SX80 as the driving endpoint, so H.265 is supported. The MX700 comes standard with two 55-inch monitors. The camera options include either a single Precision 60 camera or the Speaker Track 60 supporting two Precision 60 cameras. Another MX option is the MX800, which comes with a 70-inch monitor and a single PTZ (pan, tilt, zoom) camera. A secondary monitor can be added. Like the MX200G2 and MX300G2, the MX700 and MX800 come with a Touch 10 controller. Table 7-8 illustrates the current MX700 and MX 800 endpoints and their capabilities.

Key Topic

Table 7-8 Current MX700 and MX800 Endpoint Capabilities

Endpoint Name	Screen Size/ Resolution	Multisite	DVI and HDMI Inputs	DVI and HDMI Outputs	Audio Inputs
MX700	2x 55-inch 1920x1080	4+1 at 720p30 3+1 at 1080p30	3 HDMI 1 DVI-I	3 HDMI 1 DVI-I	15
MX800	70-inch 1920x1200	4+1 at 720p30 3+1 at 1080p30	3 HDMI 1 DVI-I	3 HDMI 1 DVI-I	15

Peripheral Device Overview

In addition to various endpoint offerings, several additional peripheral devices can be integrated into the TC software-based endpoints. The devices Cisco offers include additional microphones, cameras, and the ISDN link.

The Cisco TelePresence omnidirectional microphone uses an XLR connector and can be used with any of the C series endpoints. The Cisco TelePresence Performance MIC 20 tabletop microphone uses a minijack connector and can be used with the SX10 and SX20 endpoints. A ceiling-mounted microphone is also available, called the Audio Science MIC. This is a very small but powerful microphone centered in the middle of a noise-collection shield and has a pickup area of 15 meters.

Key Topic

Cisco Precision HD 1080p cameras come in three models, with 2.5x, 4x, and 12x zoom capability. Integrating with all TC software-based endpoints except the SX10, they all can be inverted and support full PTZ. Additional camera options include the newly designed Cisco TelePresence Precision 60 camera. This camera supports 1080p60 and has a 20x zoom capability. Two Precision 60 cameras can also be used with the Cisco TelePresence SpeakerTrack 60 dual camera option. Used in small to medium-sized conference rooms, the SpeakerTrack 60 uses voice recognition to switch between zoomed-in exposures of the speaking participant. Advanced technology in the SpeakerTrack 60 allows the cameras to triangulate the participant speaking so that if they turn away from the camera for any reason, like to write on a whiteboard, the camera keeps the participant centered in the frame.

Any endpoint that comes with the TRC5 remote can be integrated with a Touch 8 control panel. If the control panel is used on any system, the remote control is disabled. Also, the MX200G2, MX300G2, MX700, and the MX800 come with a Touch 10 controller.

Before TANDBERG came out with the C series endpoints, their premier endpoint offering was the MXP endpoints, most of which supported both ISDN communication and IP

communication over SIP and H.323. When the C series endpoints came out the need for ISDN capability native on the endpoint was less predominant, so the C series were designed to support IP communications only. Cisco wanted to reduce the number of stock-keeping units (SKUs) available to customers to prevent confusion, but there was an issue with dissolving the MXP endpoints. Many customers still required native ISDN capability on the endpoints and used MXPs exclusively. So, Cisco came out with the ISDN link. This small box contains four Basic Rate Interfaces (BRIs), one Primary Rate Interface (PRI), one V.35 serial, and two Ethernet ports. One of the Ethernet ports allows for a connection between the ISDN link and any TC software-based endpoint, and the second Ethernet port allows for a network connection between the ISDN link and the LAN network. After the ISDN link is connected to the endpoint, menu options are made available to configure the ISDN connections based on the customer's needs. This box gives ISDN capability to customers that need it without raising the cost of the endpoint for customers that do not require a native ISDN connection on the endpoint. When the ISDN Link came out, MXP endpoints were end of sale.

Cisco Intelligent Proximity for Content Sharing

In an effort to enhance the end-user experience, Cisco developed a new technology called Intelligent Proximity. Currently, there are two flavors of Intelligent Proximity. Intelligent Proximity for Mobile Voice works with 8851, 8861, and DX series phones. Intelligent Proximity for Content Sharing works with some TC software-based endpoints, specifically the MX200G2, MX300G2, MX700, MX800, and all SX endpoints. There is also support for Intelligent Proximity for Content Sharing on the IX series endpoints.

Intelligent Proximity for Mobile Voice that works with UC software-based phones enables users to sync their Apple IOS and Android smartphones and tablets with the endpoint using Bluetooth. This allows for contacts and call history on a smart device to be shared with the desktop phone. If issuers are on a call using their smartphone prior to entering their office and want to move the call to their desktop endpoint, Intelligent Proximity for Mobile Voice enables them to transfer the audio simply by selecting a button on the desk phone. The desktop endpoints transmits the audio, and the end users can continue the conversation without delay or having to press any sequence of buttons beyond the one. Note that this is using the Bluetooth technology to move the audio part of the call to the desk phone, but the call is still connected to the smartphone.

Intelligent Proximity for Content Sharing on TC software-based and IX series endpoints enables end users to use their smartphone tablet or laptop (PC and OS X operating systems only) as a remote control, of sorts, for their video endpoint. From their smart device, end users can place calls and answer incoming calls. While in a call, if the far-end endpoint shares content, Intelligent Proximity for Content Sharing enables the end user to view the content being shared on their smart device. As the far-end progresses through the content, if the end user wants to go back and view previous content being shared, Intelligent Proximity for Content Sharing provides that function to the end user. Because the ability exists to take screen captures on our smart devices, the end user also has the ability to take a screen capture of the content being shared. PCs can share content when Intelligent Proximity for Content Sharing is being used. Smartphones and tablets can download the app

from Apple Store or Google Play Store. Mac and Windows PCs must download Intelligent Proximity from Cisco.com.

Two components allow Intelligent Proximity for Content Sharing to work. This is not another Bluetooth syncing technology. This is something never before used that Cisco created. To sync a smart device with an endpoint, Intelligent Proximity for Content Sharing must first be enabled on the endpoint. The endpoint then emits a high-frequency tone through the speakers that is unnoticeable to the human ear. This ultrasound volume is set to approximately 21 kHz. This can be adjusted using command-line interface (CLI) commands on the endpoint. The smart device detects this tone and begins the synching process to the endpoint. The ultrasound is used to sync the devices, but actual communication occurs over the IP network. The second component for Intelligent Proximity for Content Sharing to work is that the smart device needs to be connected to the same network as the endpoint. Once the sync is complete, Intelligent Proximity for Content Sharing can be used on the smart device. Once established, the connection is a secure connection. A new encryption token is generated every 3 minutes to ensure the secure connection is maintained. When a device leaves the room, the connection is terminated. The distance Intelligent Proximity devices are from the endpoint they are connected to determines termination of connections. This distance setting can be changed. Intelligent Proximity for Content Sharing is still considered an experimental product at the time this writing. However, this feature works very well and is widely adopted by businesses already.

Cisco Jabber Video for TelePresence Characteristics and Installation

As discussed in previous chapters, two soft clients are available in a Cisco unified collaboration solution. The soft client discussed in previous chapters is Jabber client, which is part of the Unified Communications (UC) platform. The soft client that is discussed in this chapter is Jabber Video for TelePresence, formerly known as Movi.

Movi was originally a TANDBERG soft client. Shortly after Cisco acquisitioned TANDBERG, they rebranded Movi as Jabber Video for TelePresence to associate it as part of the Jabber soft-client platform, yet distinguish it as a separate solution from Jabber client. Jabber Video for TelePresence is a TelePresence endpoint that resides on and uses the resources of a Windows or Apple OS X-based computer. It can support high-definition video up to 1080p30, and it uses SIP SIMPLE for presence sharing.

Jabber Video for TelePresence must be provisioned to operate. The necessary components used to provision Jabber Video for TelePresence are the Cisco Video Communications Server (VCS) and the Cisco TelePresence Management Suite (TMS). TMS is the heart of where provisioning occurs. A feature must be enabled on TMS to provision called TMS Provisioning Extension (TMSPE). TMSPE requires that the Provisioning Extension application be installed first on the same server TMS resides on. Then the feature can be enabled within the TMS menus. Once this feature is enabled, several related options become active on TMS. A provisioning phonebook source and a provisioning phonebook are automatically created. For the VCS(s), there is a provisioning tab created in TMS where the VCS is managed (more on this later). The provisioning directory feature is enabled for configuring

parameters necessary for provisioning to work. In addition, TMS creates two databases: TMS Agent and SQL. This is a second sequence of SQL dedicated exclusively to TMSPE.

The first step in configuring provisioning is to establish replication between TMS and the VCS. To enable replication, the VCS must have the device provisioning option key installed. This option key enables two databases on the VCS, TMS Agent, and Open DS. To establish replication, on TMS go the **System** menu and the **Navigator** submenu. Click the VCS, and then click the **Provisioning** tab. Configure the settings displayed on this page. A visual confirmation will indicate replication is established. Figure 7-3 illustrates the provisioning configuration settings on TMS, along with the visual confirmation indicating replication has been established.

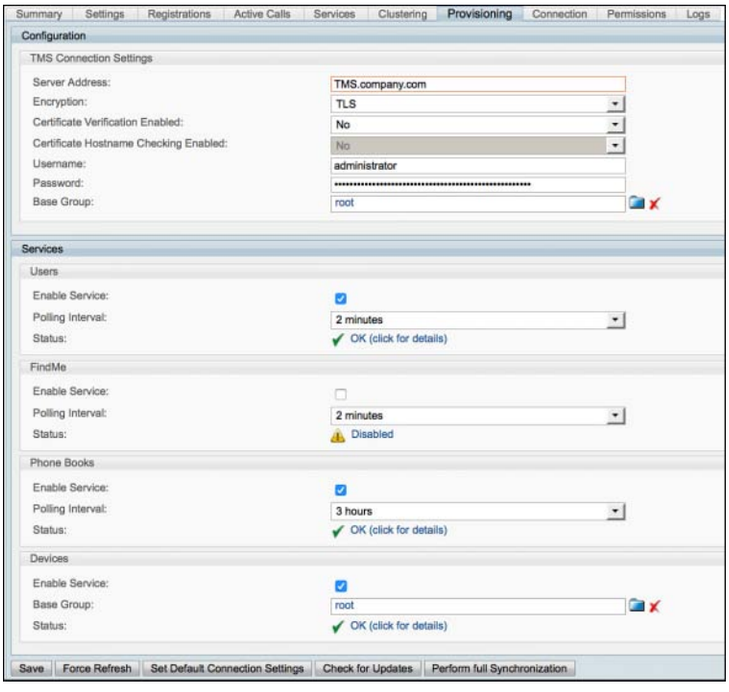


Figure 7-3 *Replication Configurations on TMS to the VCS*

Information that is replicated between the VCS and TMS include user account information, phonebooks, and the availability of provisioning licenses, which exist on TMS. This information is stored on the Open DS and SQL databases enabled with provisioning.

Once replication has been established, the next step is to configure the provisioning database on TMS. This can be found by navigating to the **System** menu and the **Provisioning** submenu. The Provisioning submenu has three options: Users, FindMe, and Devices. The Users option is where all the configurations for Jabber Video for TelePresence need to be configured. The elements that need configured here include groups, users, user settings, configuration templates, and schemas. Groups are used to segregate users based on varying privilege levels that will be assigned to them using templates. If all users will share the same

privileges, no additional groups need to be configured. User settings are the URI schemes that will be used for dialing and identifying Jabber Video for TelePresence clients. These URI patterns are template based so that they can be applied to all users within a group. Schemas are sets of configuration options based on the system type and version being used. For each schema used, a template must be configured. Templates are the configurations settings that will be applied to a group of users. Each schema must have at least one template associated with it, but schemas can support multiple templates as well. Users can be configured manually or integrated through a Lightweight Directory Access Protocol (LDAP) server, like Microsoft Active Directory (AD).

To create groups, select the **root** group, and then click the **Add Group** button at the top of the left column. When the pop-up window appears, enter the group name and click **Save**. Once a group has been created, users can be added to that group. To add a manual user, click the **Add User** button at the top of the left column. The top three fields must be configured at a minimum. They are Display Name, User Name, and Password. Click **Save** when finished. Figure 7-4 shows the Add Group and Add User buttons, along with the manual user configuration pop-up window.

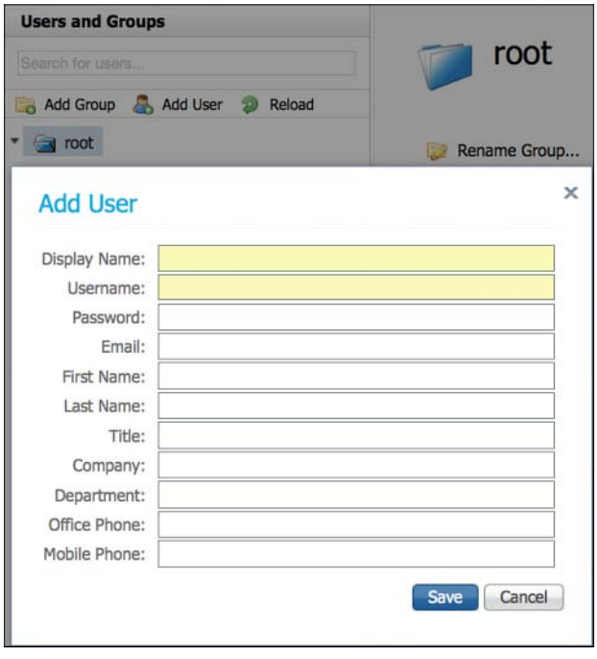


Figure 7-4 *Adding Groups and Users to TMS*

To integrate LDAP users, click the **Configure** button under the User Import menu in the right column. Select the type from the drop-down list of choices. They are Active Directory (AD), Active Directory with Kerberos (Secure AD), and Lightweight Directory Access Protocol (LDAP). Fill in the configuration fields presented on the pop-up window and click **Save**. Once complete, synchronization with the LDAP server can be initiated by clicking the **Sync Now** button. Figure 7-5 shows the configuration fields needed for AD integration.

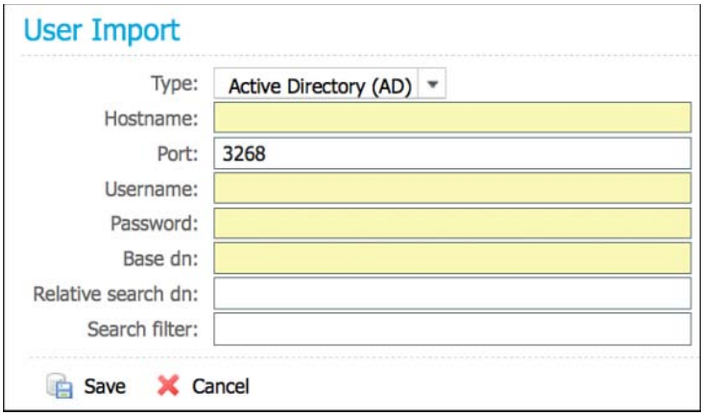


Figure 7-5 *AD Integration*

Now that groups and users have been added to the provisioning directory, user settings can be configured. In the right column, click **Edit** under User Settings. At a minimum, the video address pattern and device address pattern must be configured. The video address pattern is the address that will be displayed on a destination endpoint when in a call. The device address pattern is the address that will be used to dial provisioned devices. Typically, these patterns are configured the same. Click **OK** when finished. Figure 7-6 shows how these user settings are configured.

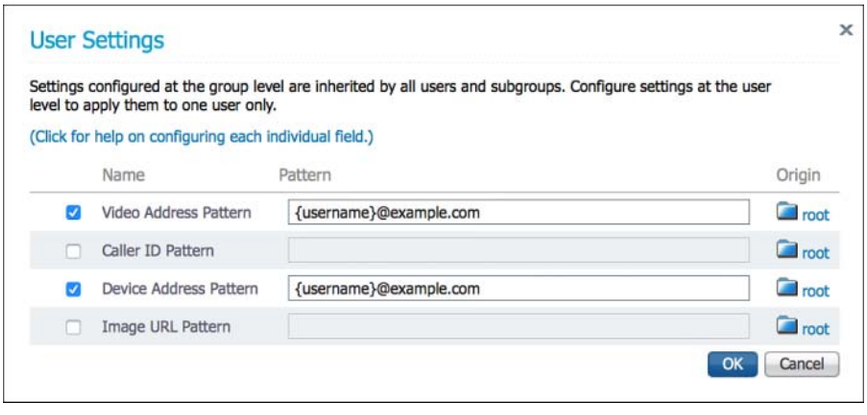


Figure 7-6 *User Settings Configuration*

Now you can add schemas. At the bottom of the left column, click the **Configuration Templates** menu. Click the **Add Schema** button at the top of the left column, browse to where the schema is located on your computer, and then click **OK**. Figure 7-7 shows how to browse for schemas.

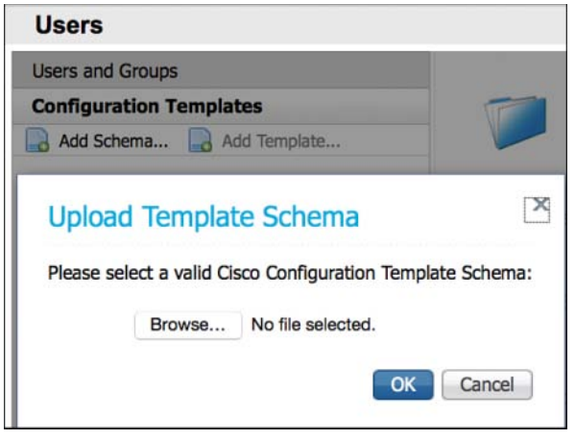


Figure 7-7 *How to Browse for Schemas*

After all schemas have been uploaded to TMS, templates can be created based on these schemas. Select a schema, and then click the **Add Template** button at the top of the left column. Configure a name for the template and click **OK**. Select the template that was just created in the right column, and click **Edit Configurations** below the Configurations section. Configure all the configuration settings needed and click **Save**. Many setting options within a template can be configured. Cisco recommends three settings be configured at a minimum. Those three settings are the SIP Server Address, Presence Server URI, and the Phone Book Server URI. Figure 7-8 shows how to configure templates.

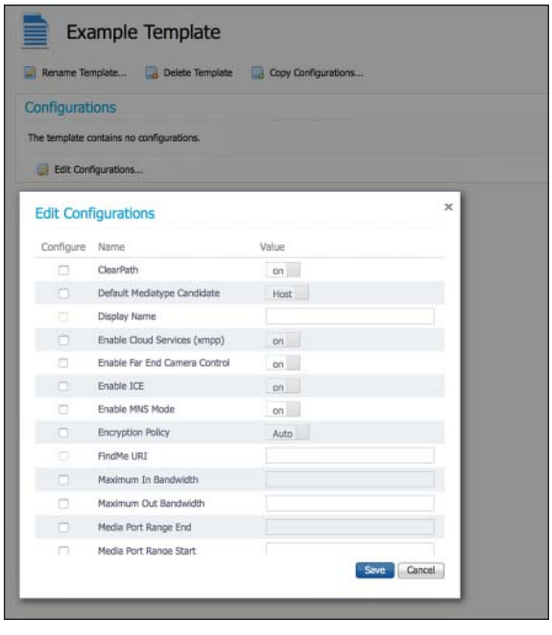


Figure 7-8 *Adding Templates to the Provisioning Directory*

Once the templates have been configured, click the **Users and Groups** menu at the top of the left column. Select a group from the list that was created in a previous step. At the bottom of the right column, click **Assign Templates** from the Configuration Templates section, check the box beside all the templates that should be assigned to this group, and click **Save**. After templates have been assigned to groups, Jabber Video for TelePresence clients are ready to be used.

After the Jabber Video for TelePresence application has been installed on your computer, open the applications and enter the username and password as they have been configured in the provisioning directory. Click the **wrench/screwdriver X** icon and select the **Sign-in Settings** menu option. Enter the IP address or the URL of the internal server (VCS Control), external server (VCS Expressway, which is optional), and the SIP domain. Click **OK** when finished, and then click the **Sign In** button when finished. After you are signed in, calls can be placed to other endpoints. Figure 7-9 shows what the Jabber client will look like after the sign-in process is complete.

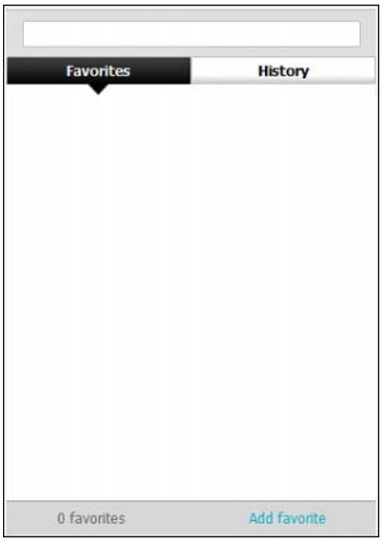


Figure 7-9 *Jabber Video for TelePresence After Sign-In*

Summary

Cisco has many endpoint solutions available that span three main software-based platforms. They are CTS software based, Android software based, and TC software based. These endpoints have a variety of different features, use two different communication protocols to communicate (SIP and H.323), and register to two different call control servers (Cisco Unified CM and Cisco VCS). Some of the key topics discussed include how TIP works using immersive telepresence room solutions with multiplexing technology for RTP and RTPC protocols. Nonimmersive CTS endpoints include the CTS 500, CTS 1100, and the TX1300 endpoints. Immersive endpoints include the TX9000 series and the new IX5000

series. DX series endpoints include the DX650, DX70, and DX80. The TC portfolio is the most expansive of the three previously mentioned software-based product lines. SX endpoints include the SX10, SX20, and the SX80. Other integrator systems include the C40, C60, and C90. Personal systems include the EX60 and the EX90. Comparisons were made between the MX200 and MX200G2, in addition to between the MX300 and MX300G2. Other MX meeting room solutions include the MX700 and the MX800. Many different peripheral devices can be used in conjunction with these TC endpoints (namely, the new and improved cameras called Precision60 cameras, which work with the SpeakerTrack dual camera option). Other great and innovative products are the Touch 8 and Touch 10 controller pads. Intelligent Proximity for Content Sharing is another great example of the leading ingenuity Cisco brings to collaboration solutions. Finally, there is the Cisco Jabber Video for TelePresence soft client that brings mobility together with Cisco's premium HD video solutions.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 7-9 lists a reference of these key topics and the page numbers on which each is found.

Table 7-9 Key Topics for Chapter 7

Key Topic Element	Description	Page Number
Paragraph	Understanding TIP and multiplexed media	161
Paragraph and table	Features of nonimmersive and immersive CTS software-based endpoints	162
Table 7-3	Features of DX series endpoints	163
Table 7-4	Features of SX series endpoints	164
Table 7-5	Features of C series endpoints	165
Table 7-6	Features of EX series endpoints	166
Table 7-7	Comparing MX200 and MX300 endpoints with the MX200 G2 and MX300 G2	166
Table 7-8	Features of MX 700 and 800 endpoints	167
Paragraph	Identifying the Precision 60 camera, SpeakerTrack and Touch control pads, and peripheral devices for TC endpoints	167
Paragraph	Explaining Intelligent Proximity for content features and functionality	168
Paragraph	Identifying the infrastructure components needed for Jabber Video for TelePresence to work	169

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

CTS, RTP, SRTP, RTCP, multiplex media, TIP, IMTC, H.265, UC, WSVGA, LCD, FHD capacitive, HDMI, DVI, EuroBlock, BNC, XLR, RCA, YPrPb, S-video, ISDN, BRI, PRI, PRI, V.35, TMS, VCS, LDAP, AD

This chapter covers the following topics:

- **Cisco TelePresence CTS Software-Based Endpoint Setup:** This section discusses three different options used to interface with the Cisco TelePresence CTS software-based endpoints.
- **Configure a Cisco TelePresence CTS Software-Based Endpoint:** This section covers the first-time setup process for Cisco TelePresence CTS software-based endpoints, how it caches DHCP addresses, how and when to use the default IP address, how to default the endpoint, and how to statically assign IP information and TFTP server addresses.
- **Calibrate a Cisco TelePresence CTS Software-Based Endpoint:** This section discusses how to run the First-Time Setup Wizard and how to calibrate the Cisco TelePresence CTS software-based endpoints.
- **Cisco TelePresence CTS Software-Based Endpoint User Accounts:** This section covers the different user accounts available on Cisco TelePresence CTS software-based endpoints, how to secure those accounts, and how to perform the password recovery.

CHAPTER 8

Configuring Cisco TelePresence CTS Software-Based Endpoints

The endpoint platform Cisco came out with that they are the proudest of is Cisco TelePresence System (CTS) software-based endpoints. Originally, the Cisco Unified Communications (UC) platform dealt primarily with Voice over IP (VoIP). The way in which the CTS endpoint was developed allows the TelePresence video endpoint to register and setup calls in the same fashion.

This chapter looks more closely at the similarities of the registration process the CTS endpoint uses to that of other UC products. Further discussion includes a beginning-to-end process demonstrating how to configure the CTS endpoint, calibrate it to the room environment, and set up and support user accounts.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 8-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 8-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Overview	1–3
Cisco TelePresence CTS Software-Based Endpoint Setup	4
Configuring a Cisco TelePresence CTS Software-Based	5–6
Calibrating a Cisco TelePresence CTS Software-Based	7–9
Cisco TelePresence CTS Software-based Endpoint User Accounts	10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following Cisco IP Phones can be used as a control device with the Cisco CTS 500-32 endpoint?

   a. 7970
   b. 8831
   c. 8945
   d. 9971

2. Which of the following Cisco Touch controllers can be used as a control device with the Cisco CTS 500-32 endpoint?

   a. Touch 8
   b. Touch 10
   c. Touch 12
   d. Touch devices cannot be used with this endpoint.

3. Which option allows for multiple TFTP servers to be discovered during the DHCP process?

   a. Option 66
   b. Option 99
   c. Option 15
   d. Option 150

4. Which of the following are ways that can be used to interface with the Cisco CTS 500-32 endpoint?

   a. CLI using Telnet
   b. CLI using SSH
   c. HTTP
   d. Console

5. Which of the following is the default IP address of the Cisco CTS 500-32 endpoint?

   a. 192.168.1.2
   b. 192.168.100.2
   c. 192.168.2.2
   d. 192.168.200.2

6. Which of the following commands will reset the Cisco CTS 500-32 endpoint but not delete any Image Slot files?

   a. **xCommand DefaultValuesSet <1-3>**
   b. **xCommand FactoryReset Confirm: Yes**
   c. **Utils System Factory Init**
   d. **Utils System Factory Reset**

7. When can the Setup Wizard be used on the CTS 500-32 endpoint?

   a. During the first-time boot or after the endpoint is reset
   b. During the first 60 seconds after the endpoint has booted
   c. Any time
   d. Any time after the endpoint is registered to the Cisco Unified CM

8. What must be used to calibrate the camera on the CTS 500-32 endpoint?

   a. Cisco PrecisionHD 1080p camera with 4x zoom
   b. Cisco PrecisionHD 1080p camera with 12x zoom
   c. Cisco Precision 60 1080p camera with 20x zoom
   d. Cisco PrecisionHD 1080p USB camera

9. What technology does Cisco use with Intelligent Proximity for Content Sharing that allows computers, smartphones, and tablets to connect with endpoints?

   a. An image on a cardboard piece that comes with the endpoint
   b. A person sitting in front of the camera
   c. A special light sensor that measures the lighting conditions of the room
   d. The automatic PTZ feature for the built-in camera

10. Which user account gives access to the CLI and web interface of the CTS 500-32 endpoint but restricts the ability to change any settings?

    a. Guest
    b. Admin
    c. User
    d. Helpdesk

Foundation Topics

Cisco TelePresence CTS Software-Based Endpoint Overview

To better understand the Cisco TelePresence CTS software-based endpoints, an understanding of how the endpoints communicate within a network is needed. CTS software-based endpoints only register to the Cisco Unified CM; therefore, the process of registering a CTS endpoint is no different from how UC endpoints communicate within a network. The focus of this chapter is on the CTS 500-32 endpoint. There are some differences to setting up other CTS software-based endpoints, primarily because they all use a camera cluster with three cameras. The immersive TelePresence solutions also use three or more monitors. Because the CTS 500-32 endpoints come with only a single camera and monitor, they can leverage a First-Time Setup Wizard as well. This Setup Wizard is available only on the CTS 500-32 endpoints, but more on that later.

The first object that needs to be identified when setting up CTS 500-32 endpoints is the control device used to interface with them. Cisco makes two options available to the customer. The first is a Cisco 7970G or 7975G VoIP phone. Alternatively, the Cisco Touch 12 can be used. The following steps outline the process a CTS 500-32 endpoint goes through to register to the Cisco Unified CM:

1. A Cisco CTS 500-32 endpoint receives power from a power cube. When a VoIP phone is used, it receives PoE from the CTS 500-32 endpoint, but both endpoints send separate communications out across the network.
2. The first message they send out is the Cisco Discovery Protocol (CDP) to the switch. This CDP communication is used to obtain the voice VLAN information.
3. Once VLAN discovery is complete, the two endpoints will a Dynamic Host Control Protocol (DHCP) Discovery message to the DHCP server. Typically the DHCP server is a router, but the Cisco Unified CM can also fulfill this role. A limitation in using the Cisco Unified CM is that it only allows support for 1000 devices. However, in either case, an option is made available for the TFTP server address to be discovered at the same time. This option is called *Option 150*. Once the DHCP server receives the DHCP Discovery, it responds with a DHCP Offer. The DHCP offer includes an IP address, subnet mask, default gateway address, TFTP server address (with use of Option 150), and possibly one or more Domain Name System (DNS) addresses. The endpoints respond to the DHCP Offer with a DHCP Request for the specific information sent in the DHCP Offer. The DHCP server then sends a DHCP Acknowledgment authorizing the use of the DHCP information exchanged and end the DHCP session.
4. Now that both endpoints have appropriate IP address information and the TFTP server address, they can send a TFTP Get message to the TFTP server. This message is typically sent over HTTP when using current endpoints, although TFTP signaling could be used as well. The communication the endpoints sent to the TFTP server contains their MAC addresses because that is what the Cisco Unified CM uses to identify the endpoint. The first element the endpoint tries to download is a certificate trust

list (CTL) file. The CTL file contains a set of certificates and is used only when Cisco Unified CM cluster security has been enabled. Next the endpoints try to download their own configuration files. After the configuration file has been downloaded, the endpoints verify they are running the requested load or firmware version. If the version they are running differs from the current version on the TFTP server or differs from a version specified in the configuration file, the endpoints then download the current system load files and upgrade the firmware. Once upgraded, the endpoints reboot. All information obtained up to this point is retained.

5. The final step in the process is for the endpoints to register to the Cisco Unified CM. The endpoints send their IP address with their alias information to the Cisco Unified CM and request registration. This is the point in the process that the endpoints communicate they will be functioning on a shared line. The Cisco Unified CM responds with a Session Initiation Protocol (SIP) message 200 OK. Now the registration process is complete.
6. If the VoIP phone is being used, it sends Extensible Markup Language (XML) messages to the Cisco TelePresence Manager (CTMan) for conference scheduling. In this case, TelePresence Management Suite (TMS) cannot be used. Without scheduling calls, the VoIP phone will place calls directly for the CTS 500-32 endpoint. Figure 8-1 illustrates a summary of this registration process using the VoIP phone.

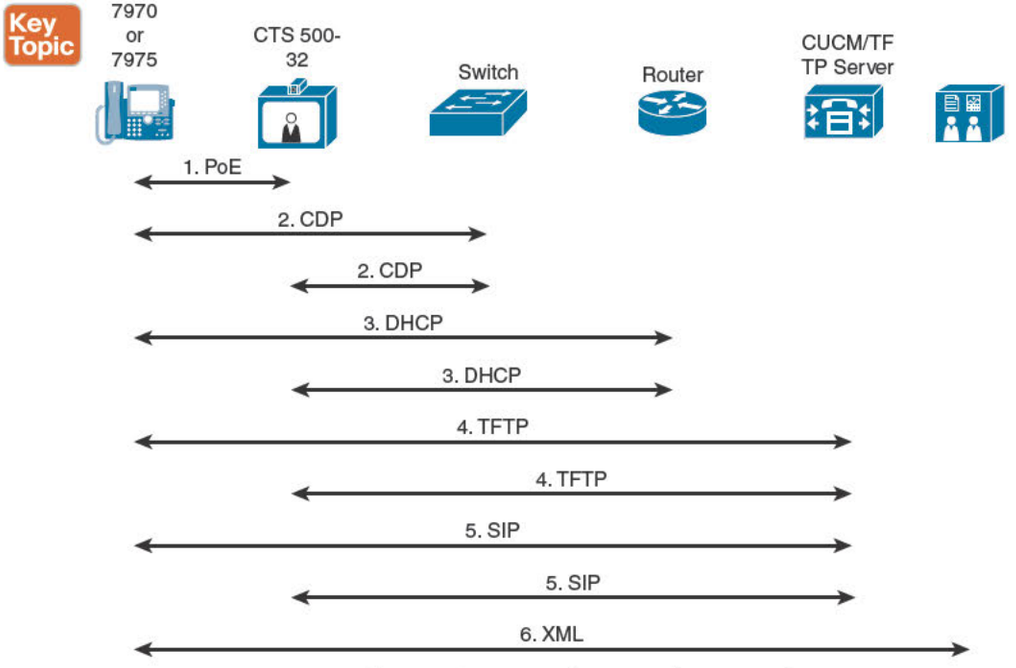


Figure 8-1 *Registering the CTS 500-32 Endpoint with a VoIP Phone*

Several limitations apply to using a VoIP phone with the CTS 500-32 endpoint. URI dialing cannot be implemented with IP Phone integrations because these phones do not support this feature. With more moving parts, several aspects could prevent either component from registering with the Cisco Unified CM. This could create a troubleshooting nightmare. Also, because the 7900 VoIP phone cannot communicate this Cisco TMS, One Button To Push (OBTP) cannot be used either. CTMan can support OBTP, but it is end of sale. The recommended device to use in conjunction with the CTS 500-32 endpoint is the Cisco Touch 12. Sporting a 12-inch touchscreen, this device is more user friendly than the VoIP phone, and the registration process is simpler. The Cisco Touch 12 receives Power over Ethernet (PoE) from the endpoint, just like the VoIP phone would. However, the CTS 500-32 endpoint alone performs all the Cisco Discovery Protocol (CDP), Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Session Initiation Protocol (SIP) communication. When the endpoint downloads the system load files, there are load files for the Touch 12 as well. The endpoint is responsible for delivering these load files to the Touch 12. Like the VoIP phone, the Touch 12 will communicate to Cisco TMS using XML to receive conference schedule information. OBTP can also be used when calls are scheduled through Cisco TMS, and URI dialing is supported. Figure 8-2 illustrates the registration process of the CTS 500-32 endpoint using the Cisco Touch 12.

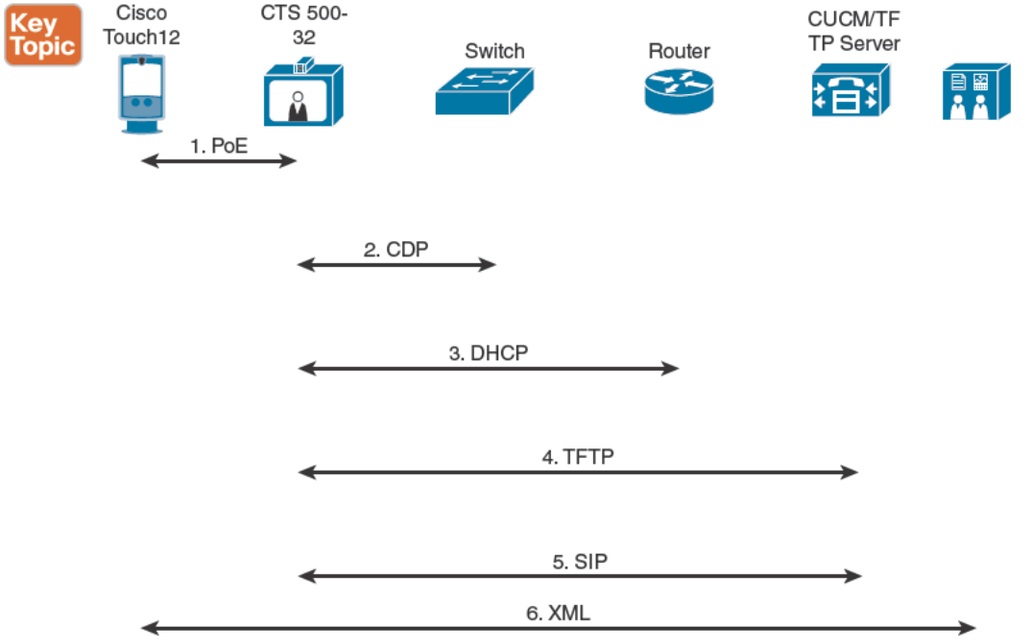


Figure 8-2 *Registering the CTS 500-32 Endpoint with a Cisco Touch 12*

For the remainder of this chapter, the discussion covers only using the Cisco Touch 12 with the CTS 500-32 endpoint, and not the VoIP phone. Before a user can configure the CTS 500-32 endpoint, it is important to understand how users can interact with the endpoint.

CTS Software-Based Endpoint Setup

A user can interact with the CTS 500-32 endpoint in three different ways:

- Using the web interface via HTTPS
- Using the command-line interface (CLI) via Secure Shell (SSH)
- Using the Cisco Touch 12.

Key Topic

The web interface of the CTS 500-32 endpoint is a great way to perform more advanced functions on the endpoint for users who are not familiar with the CLI. However, the browser that must be used is critical. The officially supported web browser that can be used to interact with the CTS 500-32 endpoint is Internet Explorer (IE) Version 6. Although you might be able to use other web browsers with this endpoint, know that there could be error messages preventing you from logging in or errors when configuring different settings within the web interface. After you first log in to the unit, you will see a menu in the left column and a menu screen to the right. The main menu headings of the menus in the left column are Device Information, Configuration, Troubleshooting, and Monitoring. Although call statistics can be monitored in real-time from the web interface, calls cannot be launched from here. Under the Device Information section, three slots identify the image loads currently stored on the CTS 500-32 endpoint. They are listed from left to right as Slot 1 Image, Slot 2 Image, and Factory Image. The image the unit will use when it boots will be highlighted with bold blue lettering. This is important to identify and understand when booting the endpoint or before performing a factory reset. Figure 8-3 shows what the web interface of the CTS 500-32 endpoint look likes.

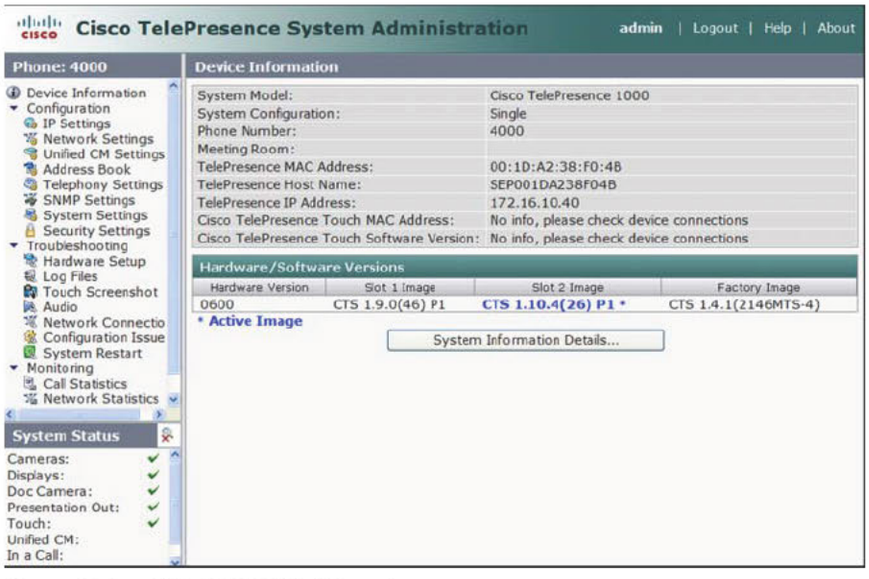


Figure 8-3 *CTS 500-32 Web Interface*

The CTS 500-32 endpoint allows users to interact with it using the CLI as well. Before using the CLI, it is important to understand that there is no Telnet support on this device, nor is there a serial or console interface. Therefore, only Secure Shell (SSH) can be used. To use SSH, you need to use an emulator, like PuTTY, to begin the session. Enter the IP address of the endpoint and click **Open**. When prompted, enter the username and password. When you see the admin: prompt, you have successfully logged in. The command structure is similar to the CLI of the Cisco Unified CM, because it is built from the same Red Hat software kernel. The **?** can be used to list commands that are less familiar. Some of the base-level commands are **utils**, **show**, **call**, and **set**. Whereas calls could not be initiated from the web interface, they can be initiated from the CLI. The third way users can interact with the CTS 500-32 endpoint is by using the Cisco Touch 12 control pad. Menu options only display on the Cisco Touch 12 after the endpoint has registered and the Touch 12 has received its system load file from the endpoint. The user options are limited on the Touch 12 as compared to the web interface and the CLI. Your average user will only need to use the control pad for basic calling functions on the CTS 500-32 endpoint. Therefore, the Touch 12 can be used to place calls, end calls, and share content. If OBTP is scheduled with the CTS 500-32 endpoint, a button will appear on the control pad to start the meeting. Users can also view call statistic information using this device.

Configuring CTS Software-Based Endpoints

You must consider several factors when setting up the CTS 500-32 endpoint for the first time. Such factors include how the endpoint obtains IP information and how it communicates with the TFTP server. In the event that the system requires a factory reset, you must consider what options exist and the impact this operation has on the endpoint. Like any endpoint that registers to the Cisco Unified CM, a phone must be configured on the Cisco Unified CM before registering the endpoint. Outside of SSH access via the CLI, there is no real security established on the endpoint itself. These security settings are configured on the Cisco Unified CM when the phone configuration file is created. This section focuses on registering the phone. Securing the endpoint is discussed in the section "CTS Software-Based Endpoint User Accounts."

By default, the CTS 500-32 endpoint uses DHCP to obtain IP address information. Should the endpoint need to be rebooted at any time, the IP information obtained during the DHCP process will be cached and reused after the reboot process is complete. When the endpoint first boots, the user will first see the Touch 12 and the monitor power on. The monitor will display the Cisco name and logo for about 60 seconds and then return to sleep mode. Meanwhile, the control pad displays circles in the lower-left corner of the screen numbered 1 through 7. These are POST tests of sorts that the endpoint uses throughout the boot and registration process. When the Touch 12 gets to the number 4 circle, the monitor wakes up again and displays its own circles numbered 1 through 6. In addition, a box on the right side of the monitor lists MAC, IP, VLAN, 802.1X, and CTS S/W. The MAC address settings and CTS S/W settings will display immediately, and the 802.1X will display *Not Required*. However, the IP and VLAN options will first appear blank. When the CDP and DHCP processes are complete, the IP and VLAN information will display. Figure 8-4 shows what the monitor might look like during a CTS 500-32 system startup.

Figure 8-4 *CTS 500-32 Monitor During System Startup*

An administrator needs to write down the MAC and IP information immediately because the information will display for only about 60 seconds. If there is an issue with registration, this information cannot be obtained from the endpoint again. Once the endpoint registers, if there are no issues, the Touch 12 control pad displays the directory number (DN) of the endpoint and a numeric dialing pad.

Key Topic

It has already been established that the CTS 500-32 endpoint uses DHCP by default; however, certain network environments do not allow for DHCP to be used. If this is the case, the endpoint has a default IP address of 192.168.100.2, as Figure 8-4 illustrates. In most cases, this IP address is not routable within the network, so IP reachability to the endpoint through the network is not possible. To change the IP assignment on the CTS 500-32 endpoint from DHCP to static, a direct connection needs to be made from a PC to the endpoint. Any regular patch cable can be used. Crossover cables are not needed here. Once the physical connection is made, the IP address on the computer needs to be changed to something within the same network mask of the endpoint. Use the subnet mask 255.255.255.0. After the network settings have been established on your computer, use a web browser to navigate to the web interface of the CTS 500-32 endpoint. From here, you can change the IP assignment from DHCP to static.

To configure a static IP address on the CTS endpoint from the endpoint, you must perform the following tasks. In the left column menu, select the menu option **IP Settings**. In the right section that is displayed, click the radio button beside **Use Static IP Address: Yes**. In the boxes provided below, configure the IP address, subnet mask, default gateway, and optionally the two DNS server addresses. Scroll to the bottom of the page and click the **Apply** button. The unit will require a system reboot before the new IP configurations can be used. If VLAN information was not discovered, these settings must be configured as well. Click the **Network Settings** menu option in the left column menus. Under Administrative VLAN ID, enter the VLAN this endpoint should use. Click **Apply** to save these settings. Figure 8-5 illustrates how to change the IP address to static and assign an administrative VLAN ID through the web interface of a CTS 500-32 endpoint.

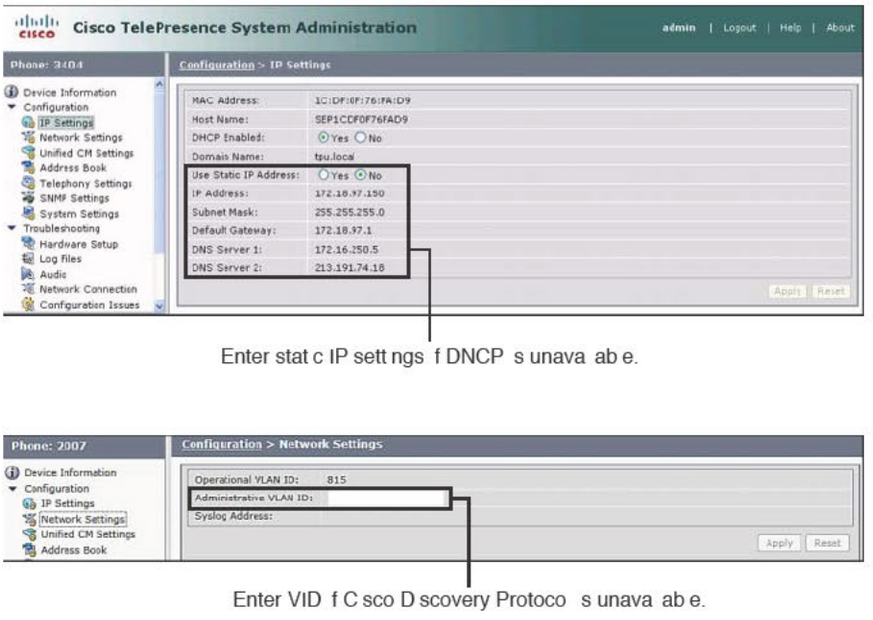


Figure 8-5 *Static IP address and Administrative VLAN ID Configurations on CTS 500-32*

By default, the CTS 500-32 endpoint uses Option 150 to discover the TFTP server address. However, if Option 150 is not being use, the TFTP server address can be manually configured on the endpoint. From the web interface in the left column menus, click the **Unified CM Settings** option. In the right section displayed, click the radio button beside **Use Configuration TFTP Servers: Specify**. Beside the TFTP Server 1 configuration box, enter the IP address of the Cisco Unified CM TFTP server address. Click the **Apply** button when configurations are complete.

Key Topic

Once a CTS 500-32 endpoint is configured and registered to a Cisco Unified CM, the endpoint can be left alone and will function without issue within its environment. However, after endpoints have been running over long periods of time, issues can be introduced that sometimes require the endpoint to be reset to factory default settings for the issues to be corrected. Two options are available that can be used to default the Cisco CTS 500-32 endpoint. Both options can be set only through the CLI of the endpoint, and you must be aware of some key differences between them.

From the CLI, the two commands that you can use are **Utils System Factory Init** and **Utils System Factory Reset**. Both commands remove any and all configurations on the endpoint and reset the factory defaults. Some of the settings that will be changed include removing any statically assigned IP settings, the IP assignment will be reverted back to DHCP if changed to static, and any cached IP information obtained from the DHCP server will be removed. Also, all TFTP server addressing information is removed, along with any information received from the TFTP server, such as DNs, passwords, calling search spaces (CSSs), device pools, partitions, and other related settings. If the TFTP mode was changed to Specify, it will be set back to Automatic.

The differences between these two commands have to do with the system load files. As mentioned before, the CTS 500-32 endpoint can store up to three image files, one being the factory image and the other two being image files download from the TFTP server during the registration process. If the **Utils System Factory Init** command is used, all these image slots are left alone, and only the other mentioned settings are defaulted back to the original factory defaults. However, if the command **Utils System Factory Reset** is used, all system load files are removed from the endpoint and the factory image slot is used. All the other configuration settings revert back to factory defaults as well. Figure 8-6 illustrates how to identify the system load files that have been downloaded to the CTS 500-32 endpoint and which image slot is being used by the endpoint.

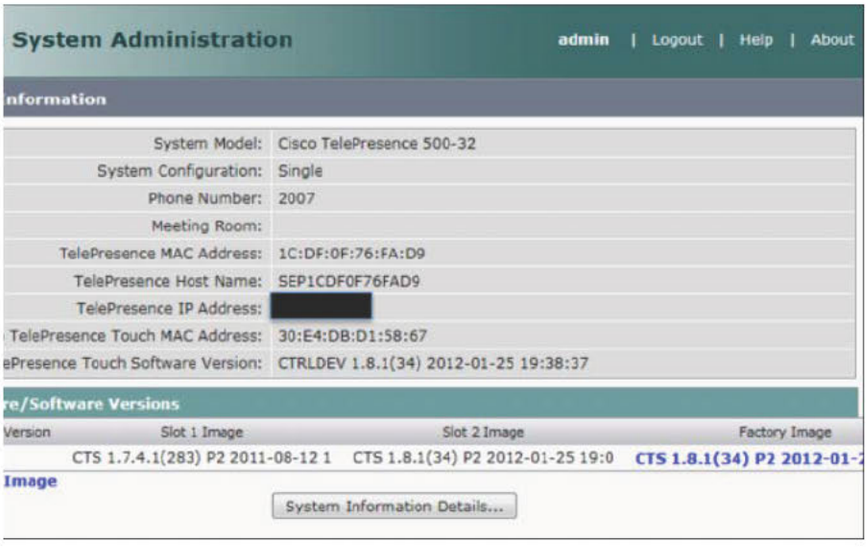


Figure 8-6 *Image Slots on the CTS 500-32 Endpoint*

Calibrating CTS Software-Based Endpoints

Key Topic

The previous section discussed to some length how to configure a CTS 500-32 endpoint. This section builds on this foundation to explain how to calibrate the endpoint for optimal performance within an office environment. Calibration of the CTS 500-32 endpoint can be performed using the First-Time Setup Wizard. Alternatively, the endpoint can be calibrated at any other given time through the menu options within the web interface. This section also discusses how these endpoints can be upgraded.

If the CTS 500-32 endpoint is being set up for the first time, a message will appear in the center of the monitor instructing you to log in to the web interface and run the First-Time Setup Wizard. This must be done before registration can be completed. With this message, the IP address will also be displayed. Open a web browser and navigate to the IP address. Figure 8-7 shows the First-Time Setup Wizard when it first appears.

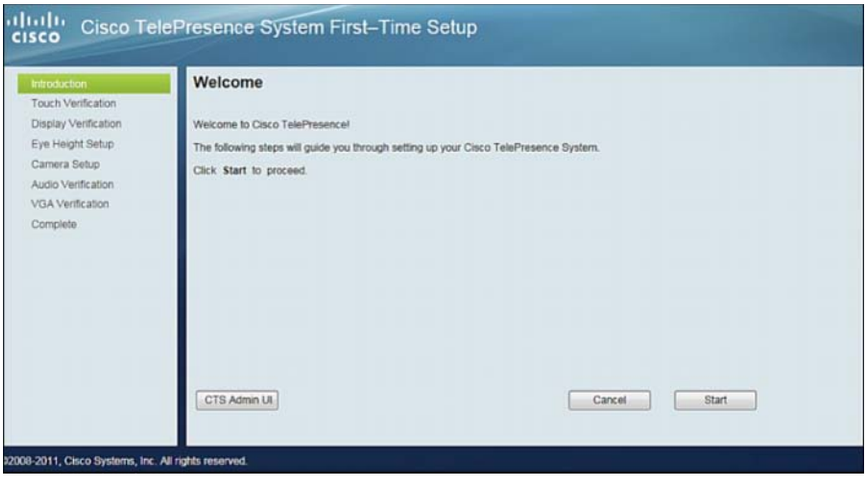


Figure 8-7 *First-Time Setup Wizard*

As you can see in Figure 8-7, the settings that this wizard will calibrate include the touch verification, display verification, eye height setup, camera setup, audio verification, and VGA verification. To start the First-Time Setup Wizard, click the **Start** button. The first setting that you need to calibrate is the Touch 12. Several buttons will appear on the touch display that you will need to "touch" to calibrate this device. Click the **Next** button when calibration of the Touch 12 is complete. The next screen is Display Verification. There will be an image on the display that should match the image on the web interface. If they match, click **Next** to calibrate the eye height setup. A red square will display on the monitor. Press the button located on the back of the pedestal the CTS 500-32 endpoint is mounted on, and elevate or lower the monitor so that a person's face would center in the red square when seated in front of the camera. Once the height is set correctly, the camera can be calibrated. This is the most difficult part of the calibration process. Locate the cardboard cutout and click **Next**. The cardboard cutout has a pattern printed on it that looks like a QR code and can be folded into a triangle. The monitor displays the same red square from the previous step. Align the cardboard cutout so that the pattern fills the inside of the red square. It is important that the cardboard cutout be very still. It is best to stack boxes or something that it can be placed on so that there is almost no movement at all. When ready, click the **Start** button from the web interface, and the camera will take a picture of the image on the cardboard cutout. That picture will display on the monitor beside an image that is should match to. If the picture is blurry and out of focus, you can manually adjust the camera to focus the picture. Pull the cover off the camera and adjust the zoom and focus of the lens. Click the **Try Again** button in the web interface to take a picture again. The camera can also be manually adjusted for pan, tilt, and horizon. There are tiny screws on the bottom of the camera that can be used to adjust these settings. When you are satisfied with the camera adjustments and the image quality, click the **Next** button. Audio verification test the built-in microphone and speakers. A meter will appear on the web interface. Speak in a normal tone and watch the needle on the meter move. Then speak very softly and verify that the microphone can still pick up your voice. Speak louder than normal to ensure the microphone can

handle louder outbursts. For the speaker calibration, the endpoint will emit the Cisco tune over the speakers. Adjust the volume so that the music can be heard at a comfortable volume. The last calibration test is the Video Graphics Array (VGA) connection. Using a VGA cable, connect a laptop computer to the endpoint. Click the **Start Presentation** button that is made available on the Touch 12. If your computer screen is displayed on the monitor, this step is compete. If not, you may want to check all your connections to ensure that the cables are seated properly. Clicking the **Finish** button circles you back to the welcome and introduction page shown in Figure 8-7. If you do not want to run the wizard, or if you did run the wizard and you are finished, you can click the **CTS Admin UI** button. This redirects you to the Web Portal login page for the CTS 500-32 endpoint.

If you opted not to run the First-Time Setup Wizard, or you want to recalibrate one of the settings, a tool is provided to perform these tasks from the web interface. After the endpoint has registered, log in to the web interface of the endpoint. In the left menu column under the Troubleshooting section, click the **Hardware Setup** option. The display field right of the menus will show all the above-mentioned calibration options. Click the option you want to calibrate, and then click the **Start** button. They can all be calibrated in the same manner as mentioned earlier.

Whether the endpoint was set up for the first time or a factory reset was performed on the endpoint, the factory image will be the boot image the CTS 500-32 endpoint will use each time. An updated image file can be loaded to the endpoint, but the factory image will still be used unless the boot slot is changed. To upgrade the endpoint, a newer version software must be uploaded to the Cisco Unified CM, and the *phone load name* of the version you want to use must be specified on the phone settings within the Cisco Unified CM. Figure 8-8 illustrates the field that needs configured on the Cisco Unified CM to specify a phone load name.

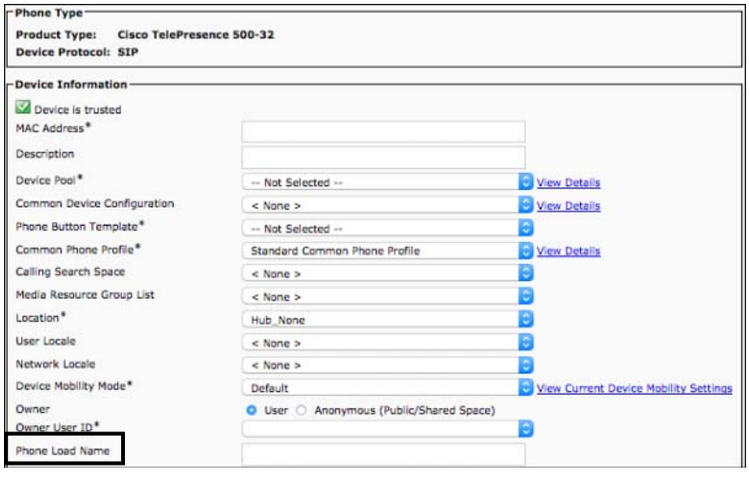


Figure 8-8 *Configuring the Phone Load Name on the Cisco Unified CM for a CTS 500-32 Endpoint*

When the endpoint requests the configuration file from the TFTP server, the TFTP server will also check whether the CTS 500-32 has the current image. If not, the system loads files are downloaded to the endpoint. Even though the endpoint receives the current image, the boot image will still be set to the factory image boot slot. To change this, open a CLI session with the endpoint. Once logged in, enter the command **Utils System Switch Version Force [1 | 2]**. The **1** or **2** will depend on whether you want to use Image Slot 1 or Image Slot 2 on the CTS 500-32 endpoint. A reboot is required to finish the upgrade. Be aware that an upgrade of the CTS 500-32 endpoint can take up to 2 hours to complete. A reboot can be initiated from the web interface, the CLI, or from the Cisco Unified CM (provided the endpoint is registered).

CTS Software-Based Endpoint User Accounts

At this point, the Cisco CTS 500-32 endpoint has registered to the Cisco Unified CM, and everything has been calibrated. However, to get to this point, an administrator must log in to the endpoint either through the web interface or through the CLI. Therefore, it is important to understand the different user accounts available on the CTS 500-32 endpoint and how to secure the endpoint from unauthorized users logging in to it.

Two different user accounts are available on the CTS 500-32 endpoint:

- The admin user can log in to the endpoint through the CLI or the web interface and has unrestricted access to every setting within the endpoint.
- There is also a helpdesk user who can also access the endpoint though the web interface or the CLI and can access everything. However, the helpdesk user cannot change any configuration settings. Only the admin user possesses this ability.

Both user accounts share the same password of cisco by default. This password cannot be changed on the endpoint. Security policies for the endpoint must be enforces from the Cisco Unified CM.

Log in to the Cisco Unified CM to secure the user accounts. From the menus across the top of the screen, navigate to **Devices> Phones**. Click the CTS 500 phone profile that has already been created, or create a phone profile for a new endpoint to be added. In the configuration menus that display, scroll down to the Secure Shell Information section toward the bottom of the page. The options available within this section include SSH Admin User*, SSH Admin Password*, SSH Admin Life*, SSH Helpdesk User*, SSH Helpdesk Password*, and SSH Helpdesk Life*. The usernames and passwords for both accounts are used to log in to the web interface and the CLI via SSH, though they imply they are just for SSH by their name. The Life setting for each user account implements a policy that will require passwords to be changed after certain duration of time. The number value represents increments of days, and 60 is the default value. This can be changed to meet an organizations internal policy requirement. If this value is set to 0, the password will never need to be changed. Figure 8-9 illustrates the Secure Shell information menus from the Cisco Unified CM.

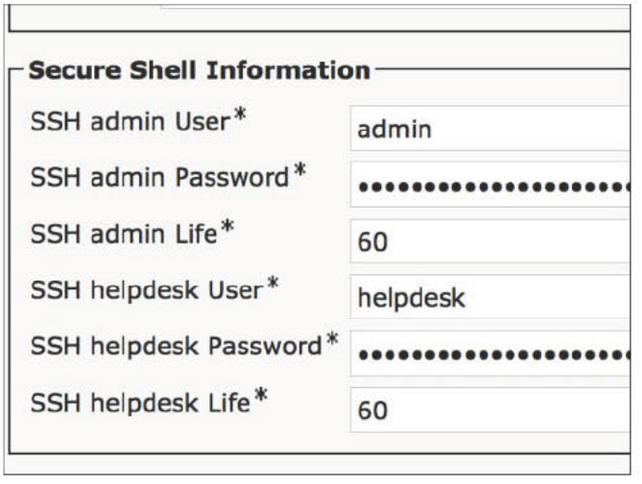


Figure 8-9 *Secure Shell Information Menus from the Cisco Unified CM*

Key Topic

If the username and password for the admin account are lost or forgotten, you can use the preceding process to reset the password. If the endpoint is not registered to the Cisco Unified CM, however, and an administrator is locked out of the endpoint, a recovery process is available to help reset the password. To use this feature, two requirements must be met:

- The administrator must have SSH access to the endpoint, meaning the laptop being used must be on the same network.
- The administrator must be in front of the unit itself. SSH into the endpoint using the CLI.

8

When prompted for the username, enter **pwrecovery**. At the password prompt, enter **pwreset**. The session will then display a warning message that you are about to reset the password and ask if you want to proceed. Type **y** for yes and press the **Return** key. On the CTS 500-32 display monitor, a code will appear. This is the reason why a password reset has to be done in front of the unit. Alternatively, someone could watch the monitor for you to retrieve the passcode. Enter the code at the prompt in the CLI session and press the **Return** key again. You will be forced out of your CLI session. The password has now been reset back to the factory password setting, which is cisco. Figure 8-10 shows what the CLI display will look like when the password recovery steps are used.

```
login as: pwrecovery
pwrecovery@10.1.5.113's password: pwreset

**********************************************
**********************************************
**                    **
** Welcome to password reset            **
**                    **
**********************************************
********************************************** Do you want to
continue ? (y/n):y Preparing the system...

Please enter the passcode:[        ] enter the passcode from the
display here
resetting admin name and password
stopping any existing admin session
admin account and password reset to default
success in applying security rules
Logging off
Connection to 10.1.5.113 closed.
```

Figure 8-10 *Password Recovery from the CLI*

Summary

For engineers who are proficient with working in a Unified Communications environment, the CTS 500-32 endpoint should feel relatively familiar. It functions much like a VoIP phone in as far as how it registers to the Cisco Unified CM. The control device used to place and disconnect calls can even be a VoIP phone, although only the 7970 and 7975 IP Phones are supported. Ideally, the Cisco Touch 12 control pad should be used with these endpoints. Either the IP Phone or the Touch 12 can be used to interface with the endpoint, along with the web interface or the CLI. The endpoint will use DHCP by default, but if there is an issue preventing the endpoint from receiving IP information, it can use the default IP address of 192.168.100.2. This address can be used to change the IP settings to static and assign the necessary addresses. The endpoint will also try to obtain the TFTP server address using Option150. If the TFTP server address is not obtained, this setting can be configured manually on the endpoint as well. Should the endpoint need reset, two options are available for issuing the factory reset. Also, the endpoint can be calibrated using either the First-Time Setup Wizard or the web interface. The two user accounts on the CTS 500-32 endpoint, the admin user and the helpdesk user, can be secured through the Cisco Unified CM. Should the password be lost or forgotten, there is also a recovery component built in to the endpoint to reset the password to its factory setting of Cisco.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 8-1 lists a reference of these key topics and the page numbers on which each is found.

Table 8-1 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Figure 8-1	Identify the process a CTS 500-32 endpoint registers with a VoIP Phone.	183
Figure 8-2	Identify the process a CTS 500-32 endpoint registers with a Touch 12.	184
Paragraph	Identify the three ways to interface with a CTS 500-32 endpoint.	185
Paragraph	Identify the Default IP address and the process of changing it to Static.	187
Paragraph	Know the process uses to factory reset the endpoint and the two options available.	188
Paragraph	Identify the two options available to calibrate the CTS 500-32 endpoint.	189
Paragraph	Identify the two user accounts available on the CTS 500-32 endpoint and how to secure the user account settings.	192
Paragraph	Know the process of performing a password recovery and the two components needed to do so.	193

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

There are no memory tables in this chapter.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

CDP, VLAN, DHCP, DHCP Discovery, DHCP Offer, DHCP Request, DHCP Ack, static, TFTP, Option150, CTMan, DN

This chapter covers the following topics:

- **DX Series Capabilities and Protocols:** This section provides an overview the capabilities of a DX series endpoint and the protocols that need to be maintained within a network to support DX endpoints.
- **DX series User Interface:** This section examines how to navigate the user interface on the DX series endpoints. Navigation will include using the app store, accessing the settings menus, and managing the user interface for placing and receiving calls.
- **Configuring Cisco DX Series Endpoints:** This section examines the different settings that need to be configured on the DX series endpoints before they can register with the Cisco Unified CM.
- **Registering Cisco DX Series Endpoints:** This section explains how to set up the Cisco Unified CM so DX series endpoints can register.

CHAPTER 9

Configuring Cisco DX Series Endpoints

What does an end user look for in a desktop video endpoint? With today's standards the first and foremost component is the ability to place high-definition (HD)-quality video and stereo-quality audio calls. Ideally, this epitomized endpoint would serve a purpose beyond video collaboration calling, such as act as a dual monitor for a computer while not in a call. Contacts should be easy to add and access for quickly calling common contacts. These, along with many other features, are considerations Cisco used to design the DX series endpoints. Smartphones are dominating the digital world, allowing users to perform tasks that surpass simply placing a phone call. By giving the DX series endpoints an Android-based operating system (OS), Cisco has been providing this same functionality within these endpoints, from downloading and using apps, to accessing the Internet.

This chapter discusses some of the different capabilities and protocols that define the DX series. You will also learn how to use this unique user interface. So that you can register a DX to a call control server so that calls can be sent and received, this chapter also explains explanation how to configure the DX series endpoint and the Cisco Unified Communications Manager (CM).

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table X-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 9-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
DX Series Capabilities and Protocols	1–3
DX series User Interface	4–5
Configuring Cisco DX Series Endpoints	6–8
Registering Cisco DX Series Endpoints	9–10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following features are not supported on the DX series endpoints?
   a. IM and Presence with Cisco Jabber
   b. Extension Mobility
   c. Visibility to call statistics
   d. Access to cloud services
2. There are three main capabilities on Cisco DX series endpoints. Which of the following is not a capability?
   a. Register to the Cisco Unified CM only
   b. Register to the Cisco Unified CM and the Cisco VCS
   c. Access to Android-based applications through Google Play
   d. Administrative control over access to applications
3. Which of the following is a protocol Cisco DX series endpoints support?
   a. LDAP
   b. H.323
   c. SCCP
   d. LLDP-MED
4. When resetting a Cisco DX series endpoint using the applications settings menu, which of the following is required?
   a. Web access to the endpoint.
   b. SSH access to the endpoint.
   c. PIN or password for the endpoint.
   d. Nothing is required.
5. When resetting a Cisco DX series endpoint using the key-press sequence, what is the correct order keys need to be pressed?
   a. 123456789*0#
   b. #0*987654321
   c. **#**
   d. ##*##

6. Which Cisco DX series endpoint supports PoE?

   a. DX650.
   b. DX70.
   c. DX80.
   d. All DX endpoints support PoE.

7. How does a DX series endpoint connect to a smartphone using Intelligent Proximity for Mobile Voice?

   a. High-frequency tone emitted through the phone's speakers
   b. Over a network connection
   c. Through a Bluetooth communication
   d. Using a secret technology Cisco has code named Pixie Dust

8. When setting up a PIN or password on Cisco DX series endpoints, what is the required minimum length?

   a. 4 digits or characters
   b. 4 digits for PINs and 8 characters for passwords
   c. 8 digits or characters
   d. 8 digits for PINs and 4 characters for passwords

9. How does a Cisco Unified CM identify an endpoint when the endpoint is trying to register?

   a. By the endpoint's IP address
   b. By the endpoint's MAC address
   c. By both the IP address and MAC address
   d. By the endpoints serial number

10. Calling search spaces are often used on the Cisco Unified CM to administer call control over phones and other systems. What other setting on the Cisco Unified CM must be configured in conjunction with calling search spaces?

    a. Device pools
    b. Regions
    c. Route lists
    d. Partitions

Foundation Topics

DX Series Capabilities and Protocol

Key Topic

The Cisco DX series endpoints are next-generation endpoints that deliver powerful, high-quality communications and collaboration for a variety of office environments. The Cisco DX series endpoints provide native support for HD video up to 1080p30 using the video codec H.264. They also support the annex codec H.264 AVC for HD video at even less bandwidth. The built-in audio speakers offer a premium-quality audio experience. For those more private calls, the attached handset can be used. Better yet, you could be hands-free by plugging in a USB wideband audio headset or standard USB headset or by connecting a Bluetooth headset. Additional features of the Cisco DX series endpoints include conferencing with Cisco WebEx meeting applications, presence, and instant messaging with the Cisco Jabber messaging integration platform. On-demand access to cloud services is always available using the Cisco DX series endpoints. With Extension Mobility (EM), any user can log in to, and use, any Cisco DX series endpoint within an organization. All personal settings are reflected on the phone after the user has successfully signed in. Table 9-2 outlines some of the features available on the DX series endpoints.

Table 9-2 DX Series Feature Comparison

Features	DX650	DX70	DX80
Full unified communications (UC) and security, Security Enhanced (SE) Android	Yes	Yes	Yes
Jabber/WebEx native support	Yes	Yes	Yes
Third-party native support (Google Play)	Yes	Yes	Yes
Max video performance	1080p30	1080p30	1080p30
HDMI in (content sharing, PC monitor)		Yes	Yes
HDMI out (external monitor support)	Dual independent display	Mirror mode only	Reserved for future use
Content viewing via Binary Floor Control Protocol (BFCP)	Yes	Yes	Yes
Document camera		Yes	Yes
Multitouch monitor	7-inch, 1024x600	14-inch, 1920x1080	23-inch, 1920x1080
PoE (Power over Ethernet)	Yes		
Mounting option	ADA wall mount	VESA adapter and mount	VESA adapter and mount
Intelligent audio feature			Yes
Global list price (GLP, in U.S. $)	$1695	$2750	$3990

Chapter 7, "Cisco TelePresence Endpoint Characteristics," introduced the concepts of the Cisco DX series endpoints. This chapter dives deeper into the nuts and bolts of how to operate a DX series endpoint within a collaboration environment. Figure 9-1 offers a graphical representation of the three different products available in the Cisco DX series endpoint platform: the DX650, DX70, and DX80.

Figure 9-1 *DX Series Endpoint Products Available*

Key Topic

Although DX series endpoints have many capabilities, three main capabilities warrant a deeper discussion:

- DX series endpoints can only register with the Cisco Unified CM via Session Initiation Protocol (SIP).
- The Android platform that drives the DX series endpoints allows users to download and use applications on their DX endpoint, just as they would on their smartphone or tablet.
- An administrator can control how a DX series endpoint can be used within a network environment and to what access to functions the end user has.

For security purposes, the DX series endpoints require a password or PIN to be set once they register with the Cisco Unified CM. When an endpoint is waken from sleep mode, the PIN must be configured before calls can be placed. Answering an incoming call is possible without entering the PIN. The monitor is a touch controller, so a user can select any part of the screen where options appear. Should number, letters, or characters need to be entered, a numeric keypad, or a QWERTY keyboard, will display on the monitor. What if you do not like to use the touchscreen keyboard? Plug in an external keyboard and mouse. Placing calls from the DX series endpoints is as easy as placing a call from an Android phone because it is, well, an Android phone. From the main screen, users can select the phone handle icon from the touchscreen. This brings them to the call page. From here, they can either select a contact from their directory or they can dial the alias of the endpoint they want to call. If that alias is a URI, selecting the keyboard icon at the bottom of the screen will bring up the QWERTY keyboard. Figure 9-2 shows the main screen and the call screen, with and without the keyboard.

Figure 9-2 *Calling Interface of a Cisco DX650*

In the top-right corner of the Cisco DX series endpoint, six dots are grouped together. Selecting these dots takes an end user into the applications page. Some useful apps are already preloaded on DX series endpoints. Some of the valuable tools presently available include a browser app for surfing the Web. Selecting this app opens a web page linked to Cisco.com. Because this is an Android-based phone system, several Google apps are preloaded onto the endpoint. Google+, Hangouts, and Maps are among the few, in addition to a Google Settings app that enables users to easily modify their Google settings. Additional apps can be added through Google Play. Other useful apps for the workplace include contacts, e-mail, and Jabber IM. Swiping the screen from right to left takes a user to additional apps, widgets, and tutorials that help explain how the tools available with the DX series endpoints can be used and leveraged for a more productive work environment. Figure 9-3 shows the Apps page on a Cisco DX650 endpoint.

Figure 9-3 *Apps Page on a Cisco DX650*

With an endpoint this feature rich, many organizations may understandably have a concern that their employees will abuse these functions and download games to their phones, or leverage it in some other nonproductive fashion. The world has suffered enough from Candy Crush. As Benjamin Franklin said, "An ounce of prevention is worth a pound of cure." Cisco has taken preventive steps to allow corporations to customize what end users are allowed to access on their Cisco DX series endpoint. Cisco offers security at multiple levels of the network. Security Enhanced (SE) Android provides more protection by isolating applications to keep sensitive data safer. And your IT admin has the option to limit device capabilities. Some of the functions on the Cisco DX series endpoints that can be administratively disabled include Google Play, Wi-Fi, Bluetooth, installation of apps from unknown sources, and USB ports. On a Cisco DX650, you can enable phone-only mode to provide the following limitations:

- The user is limited to the home screen, phone application, Contacts application, and Settings application.
- The user cannot add shortcuts or widgets to the home screen.
- Any contacts that are saved to the Contacts application in phone-only mode are stored locally and will not sync to any server.
- USB storage devices and SD cards are not supported.
- Any previously configured account data is hidden from the user when the phone enters phone-only mode.
- The phone reboots when you switch from standard profile to phone-only mode, or from phone-only mode to standard profile.

There are two operating modes for the DX series endpoints: simple and enhanced. Simple mode offers the following features and limitations:

- User cannot modify wallpaper (supports admin-assigned wallpaper).
- User can not move/add shortcuts or widgets, launch applications, or long click.
- No Android applications are allowed, and Google Search is removed.
- External USB storage is disabled.
- User can create and store local contacts.
- Bluetooth contacts and history sharing is also allowed.
- Enhanced mode enables user access to all collaboration goodies, including Jabber, WebEx, Exchange, and Google Play.

Note For more information about what can be controlled on Cisco DX series endpoints, go to http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/desktop-collaboration-experience-dx600-series/white-paper-c11-731685.html.

Key Topic

In addition to all the features Cisco DX series endpoints support, there are many protocols they support as well. These protocols are the same as other Cisco unified communications and collaboration endpoints. Cisco Discovery Protocol (CDP) is exchanged between a Cisco Catalyst switch and Cisco DX series endpoint to learn the voice VLAN ID. The endpoint sends all control and media traffic to the voice VLAN or to any other tagged IEEE 802.1Q VLAN if the connected switch is incapable of a voice auxiliary VLAN. Dynamic Host Configuration Protocol (DHCP) provides the Cisco DX series endpoint with IP addressing information and Option 150, which carries the IP address of Cisco TFTP server. If the DHCP server or Option 150 is unavailable, you can configure these settings manually. TFTP can be used to download the configuration to the Cisco DX650 endpoint and upgrade the endpoint firmware, if necessary. The Cisco DX650 endpoint is a SIP endpoint. The endpoint uses SIP to register with Cisco Unified Communications Manager and to communicate all call-setup and call-feature requests.

DX Series User Interface

So far, it has been established that the Cisco DX series endpoints have the touch-directed ease of use of an Android and the ability to personalize experiences with customizable home screens, communications widgets, ring tones, and more. The Cisco DX650 has many "smart" features and attributes. A familiar Android user interface provides users with easy, instant access to critical applications. The ability to create multiple unique user profiles can be achieved using EM. Each profile can easily integrate with e-mail, calendar integration, full directory of contacts, and speed dials for the user. Applications such as Cisco Jabber, WebEx, and AnyConnect are preloaded on the phone, making the Cisco DX series endpoints a highly versatile and productive tool for any enterprise.

Occasionally, you might need to perform a reset on a Cisco DX series endpoints that you are deploying. You perform a reset of the Cisco DX series endpoints to reset or restore various configuration and security settings or recover the device if it encounters an error. There are two ways to perform a factory reset on the DX650. You can use the application Settings menu if the device is secured with a PIN or password lock and you know the PIN or password. You should use the *key-press sequence* method if the device is secured with a PIN or password lock and you do not know the PIN or password.

Key Topic

If you are using the application Settings menu to reset the system, follow these steps:

Step 1. From the home screen, tap the **Application** button and then tap **Settings**.

Step 2. Choose the **Backup & Reset** menu option, and then choose **Factory Data Reset**.

Step 3. Enter the PIN or password for the endpoint to proceed with the reset. If the pin or password does not work, use the key-press sequence to reset the system.

Key Topic

If you are using the key-press sequence to reset the system, follow these steps:

Step 1. To turn off the device, hold the **Lock** button until it powers off. Press and hold the **#** key, and press the **Lock** button to turn on the device.

Step 2. Do not release the # key until the Message Waiting Indicator (MWI) flashes red once then stays lit. Now you can release the # key.

Step 3. In this exact order, press the **1**, **2**, **3**, **4**, **5**, **6**, **7**, **8**, **9**, *, **0**, # keys.

If successful, the MWI will flash three times to indicate that user data is being cleared. The device then continues the normal boot process.

Configuring Cisco DX Series Endpoints

Key Topic

Now that you have a basic understanding of the Cisco DX series endpoints, next you need to know how to configure the DX endpoints. Cisco DX series endpoints register exclusively to the Cisco Unified CM. The endpoint must first power on and load the locally stored image. Then the first communication it sends out is a VLAN discovery, which uses CDP in a complete Cisco environment. Once the VLAN discovery process is complete, the endpoint uses DHCP discovery to obtain IP address information. In environments where IP information is assigned statically, this part of the process will not occur. The next step is for the endpoint to communicate with the TFTP server to obtain system configuration information for registration. The TFTP server address can either be discovered through the DHCP process or it can be manually configured. Once TFTP communication is complete, the endpoint sends its IP address with the directory number (DN)/URI address to the Cisco Unified CM for registration. When the Cisco Unified CM responds with a 200 OK SIP response, the registration process is complete. The Cisco DX650 is the only DX series endpoint that supports 802.3af PoE. The Cisco DX70 and the Cisco DX80 require a power cube to supply adequate power. However, all products do support an Internet connection over either a physical LAN line or Wi-Fi. Also, Cisco DX series endpoints only support SIP. There is no Skinny Client Control Protocol (SCCP) support on these products.

The Cisco DX series endpoints obtain operational VLAN ID through CDP if the switch is also a Cisco product. Otherwise, the Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) open source protocol is used for VLAN discovery. This information comes from the switch to which the endpoint is attached. If the endpoint is connected to the network via Wi-Fi, or a voice VLAN is not configured on the switch, VLAN configuration settings will need to be configured manually. Follow these steps to assign a voice VLAN ID manually, using the Admin VLAN ID option. Use the Admin VLAN option only if the Cisco DX series endpoints do not receive an operational VLAN from the switch. From the home screen, tap the **Application** button, and then launch the **Settings** application. Choose the **Ethernet** menu and the **Admin VLAN** submenu. Enter the desired VLAN and save the changes.

When a Cisco DX series endpoint is first set up, IP information is gathered using DHCP by default. Cisco recommends that you use DHCP Option 150 to obtain the TFTP server IP address as the optional value. If you cannot use Option 150, you may try using DHCP Option 66. The main difference between Option 150 and Option 66 is that whereas Option 150 can support multiple TFTP IP addresses or URLs, Option 66 can support only a single IP address or URL for the TFTP server. As an alternative to using DHCP within an organization's internetworked environment, DHCP can be disabled, at which time you must manually configure a static IP address, subnet mask, and gateway locally on each phone. Follow

these steps to manually configure the IP settings on Cisco DX series endpoints. From the home screen, tap the **Application** button and launch the **Settings** application. Choose the **Ethernet** menu and the **IPv4 Configuration** submenu. Check the box beside **Use Static IP**, enter the desired IPv4 settings, and save the changes.

TFTP enables the phone to obtain a configuration file that is specific to the phone type. The DHCP server automatically assigns the TFTP server address if Option 150 is used. Circumstances that may constitute manually configuring the TFTP server address could be that Option 150 is not being used, the Cisco DX series endpoint is using Wi-Fi to connect to the network, or you want a phone to use a TFTP server other than the one that the DHCP server specifies. Follow these steps to manually configure the TFTP settings on Cisco DX series endpoints:

Step 1. From the home screen, tap the **Application** button and launch the **Settings** application.

Step 2. Choose the **More** menu and the **TFTP Server Settings** submenu.

Step 3. Check the box beside **Use Alternate TFTP Server**; enter up to two TFTP server addresses and save the changes.

With Cisco Intelligent Proximity for Mobile Voice, users of the Cisco DX series and select models of the Cisco IP Phone 8800 series can use Bluetooth to wirelessly sync iOS and Android mobile devices when they come in close proximity of these endpoints. Cisco DX series endpoints supports Bluetooth 3.0. You can use a Bluetooth enabled device up to 30 feet (10 m) away from your phone. For best performance, however, Cisco recommends that you use Bluetooth devices within 10 feet (3 m) of the phone. When the mobile device is out of range of the Cisco DX series endpoints, shared contacts are deleted unless you have chosen to save them, and the mobile device call history is not shown on the DX series endpoints. To configure Cisco Intelligent Proximity for Mobile Voice, ensure that Bluetooth is enabled on your mobile device. From the home screen of the Cisco DX series endpoint, tap the **Application** button and launch the **Settings** application. Toggle the **Bluetooth** setting to **On**. Tap a device to pair from the available Devices list. Verify the passkey and tap the **Pair** button. Complete the pairing request on your mobile device.

As mentioned earlier, when setting up the endpoint for the very first time, you are prompted to create a PIN or password for security after the endpoint registers. When you are prompted to set a PIN or password, tap the **OK** button and then tap the **PIN** button. Enter a PIN and tap the **Continue** button. Your PIN must be at least four digits long. Enter your PIN again and tap the **OK** button to confirm your PIN. Follow these steps to create a password. Alternatively, when you are prompted to set a PIN or password, you could tap the **OK** button and then tap the **Password** button. Then enter a password and tap the **Continue** button. Your password must be at least four characters long. Enter your password again and tap the **OK** button to confirm your password.

Registering Cisco DX Series Endpoints

Following the steps in the previous section does not mean that your DX series endpoints will necessarily register with the Cisco Unified CM. Certain settings must be configured on the Cisco Unified CM before the endpoint can register. These settings could be configured before the endpoints are configured, or after. Either way, both parts must be configured before an endpoint can register. Best practice is to configure the Cisco Unified CM first and then set up Option 150 and let DHCP deliver the TFTP addresses to the Cisco DX series endpoints. After all this is set up, simply cabling up and powering on the endpoint is all that needs done for the endpoint to register. Everything else happens "behind the curtain," so to speak. Phones can be added to the Cisco Unified CM manually, or bulk registration templates can be set up for auto-registration. Cisco also offers a new feature called the Self-Provisioning Portal that allows end-users to set up their own phones. This new, robust tool has already been widely adopted within organizations, and a lot of positive feedback has been streaming in attesting to its ease and usefulness within enterprises across the globe. You can find more information about how to provision endpoint using each of these options in the *CCNA Collaboration CICD 210-060 Official Cert Guide*. For the purpose of introducing the settings that need to be configured at a minimum on the Cisco Unified CM, this section of the book focuses on how to configure a manual phone for the Cisco DX series endpoints.

You manually add the endpoints into Cisco Unified CM Administration using the Phone Configuration windows. To add an endpoint to Cisco Unified CM, open a web browser and navigate to the Cisco Unified CM IP address or URL. Enter the username and password to log in. Scroll over the Device menu and select the **Phone** submenu option. Click the **Add New** button. From the Phone Type drop-down list box, choose the appropriate Cisco TelePresence type or device; in this case, it is the DX650, DX70 or DX80. Then click **Next**. Enter the appropriate data for the endpoint, such as the MAC address of the device, description, phone number, and any other required fields. Only those fields that are appropriate to the chosen device type are displayed in the data entry window. Click **Save** when you are done entering data. After the settings have been saved, a line directory number (DN) needs to be created; otherwise, registration will fail. Figures 9-4 through 9-8 illustrate some of the menu options available for the DX series endpoints on the Cisco Unified CM.

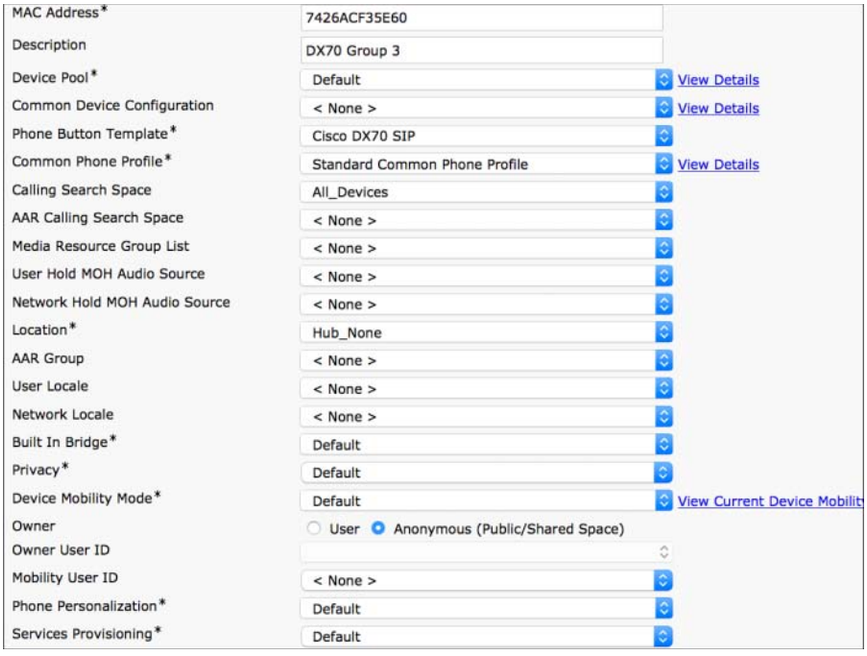


Figure 9-4 *Cisco Unified CM Options for DX Series Endpoints, Screen 1*

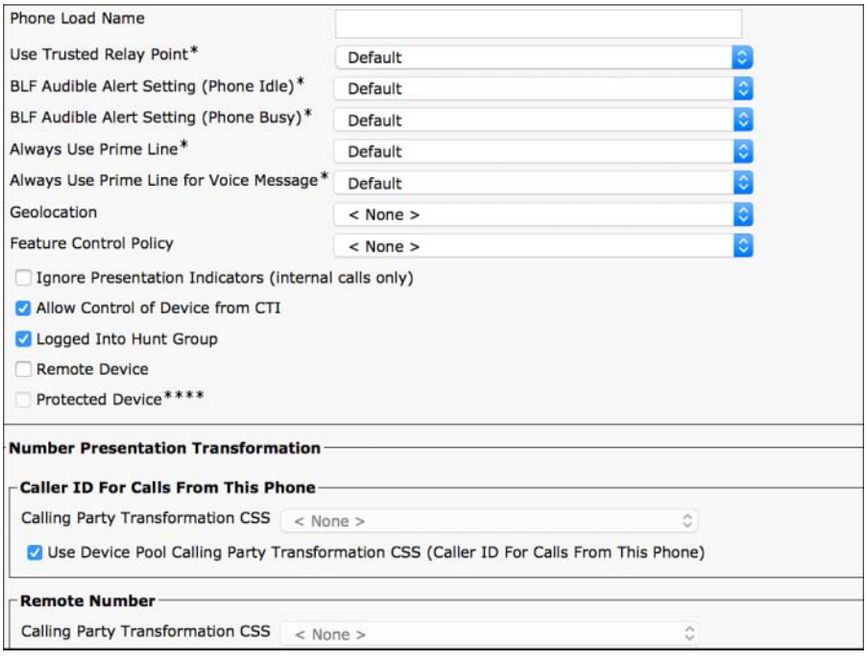


Figure 9-5 *Cisco Unified CM Options for DX Series Endpoints, Screen 2*

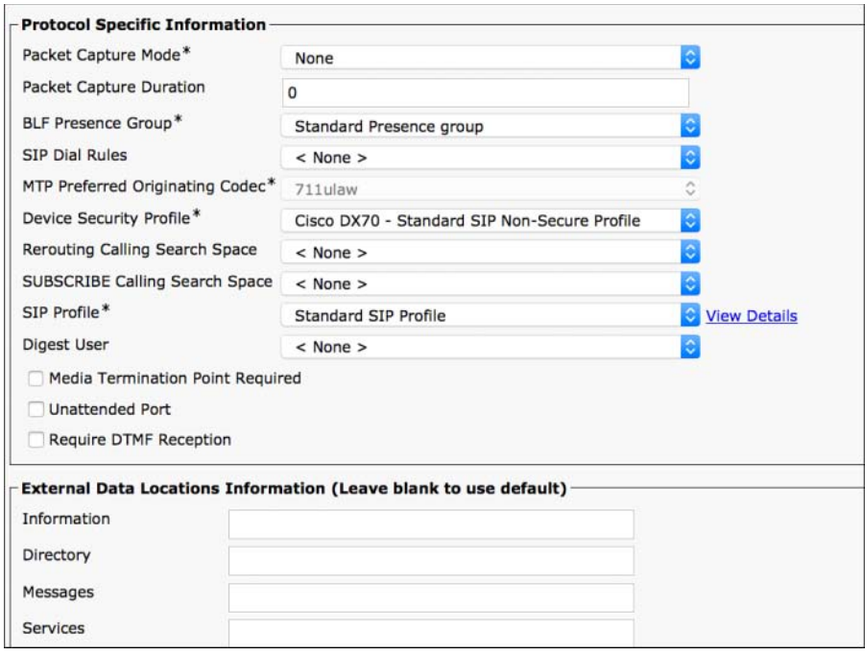


Figure 9-6 *Cisco Unified CM Options for DX Series Endpoints, Screen 3*

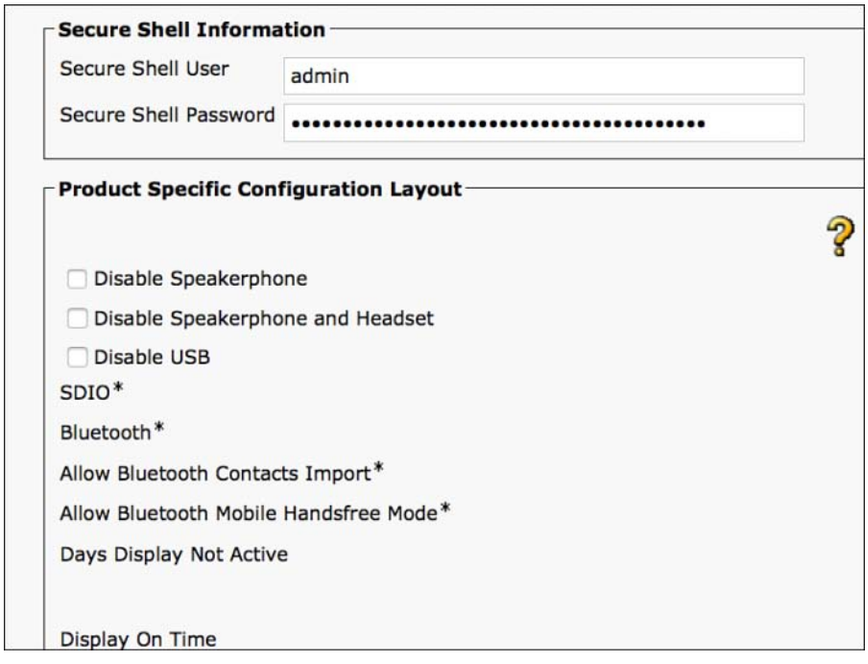


Figure 9-7 *Cisco Unified CM Options for DX Series Endpoints, Screen 4*

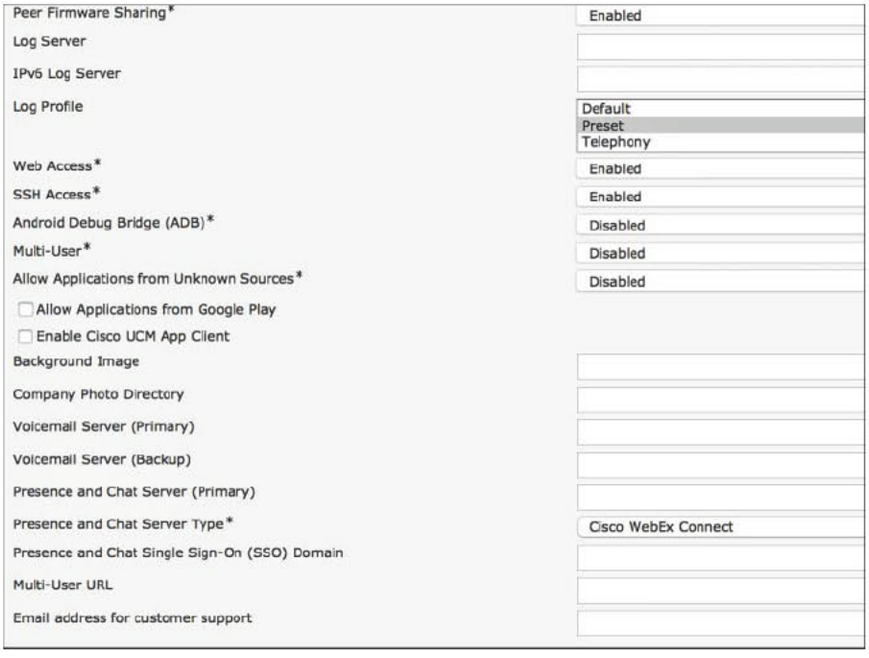


Figure 9-8 *Cisco Unified CM Options for DX Series Endpoints, Screen 5*

Because there are several different configuration settings that could be configured, Table 9-3 highlights some of the more important options available under Phone Configuration, with a brief explanation about the setting and whether the setting is required for the endpoint to register with the Cisco Unified CM.

Key Topic

Table 9-3 Phone Configuration Settings on the Cisco Unified CM

Phone Configuration Setting	Description	Required for Registration (Yes or No)
MAC address	Unique identifier used by the Cisco Unified CM to identify the device when communication is initiated through the TFTP service.	Yes
Device pool	Device pools define sets of common characteristics for devices. The device pool structure supports the separation of user and location information. The device pool contains only device- and location-related information.	No
Phone button template	When adding phones, you can assign one of these templates to the phones or create a new template. Creating and using templates provides a fast way to assign a common button configuration to a large number of phones.	Yes

Phone Configuration Setting	Description	Required for Registration (Yes or No)
Calling search space (CSS)	Partitions can be seen as a collection of route patterns. DNs, route patterns, and translation patterns can all belong to specific partitions. Calling search spaces are an ordered list of route partitions, and they determine which partitions calling devices must search when they attempt to complete a call.	No
Owner	In Cisco Unified CM Version 10.0 and later, an owner of a phone must be identified. Who the owner of a phone is can be specified under the owner user ID, or this setting can be changed to anonymous (public/shared space).	Yes
Owner user ID	This setting identifies who the owner is of this phone.	No
Phone load name	This setting is used to identify a specific firmware version the TFTP server is to use when a device tries to register.	No
Allow control of device from CTI	The Computer Telephony Integration (CTI) control service on the Cisco Unified CM allows a phone to be controlled by the Jabber soft client, meaning that when Jabber sends or receives a call request, the media and signaling are rerouted through the associated phone.	No
Device security profile	To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. Only the security features that the selected device and protocol support display in the Security Profile Settings window.	Yes
SIP profile	SIP profiles change SIP incoming or outgoing messages so that interoperability between incompatible devices can be ensured. SIP profiles can be configured with rules to add, remove, copy, or modify the SIP Session Description Protocol (SDP).	Yes
Secure Shell user	Cisco Technical Assistance Center (TAC) uses Secure Shell for troubleshooting and debugging. Contact TAC for further assistance.	No
Secure Shell password	Cisco TAC uses secure shell for troubleshooting and debugging. Contact TAC for further assistance.	No
Web access	This setting is specific to the DX series endpoints. Web access must be enabled for administrators to access the web interface of DX endpoints. The web interface allows access to important log information.	No

Phone Configuration Setting	Description	Required for Registration (Yes or No)
SSH access	This setting is specific to the DX series endpoints. SSH access must be enabled for administrators to access the command-line interface (CLI) of DX endpoints. The CLI allows access to important log information and allows administrators to issue certain commands for testing, configuring, and troubleshooting DX endpoints.	No

You can find more information about all these settings, and many more, in the *CCNA Collaboration CICD 210-060 Official Cert Guide*. From the **Device > Phones** screen, you can verify the registration status of the endpoint. The status should show Registered, along with the IPv4 address of the endpoint. If the device fails to register, click the **Device Name** link to confirm that you correctly entered the MAC address of the endpoint and that the phone has a line DN. These are common reasons an endpoint will not register.

Summary

The Cisco DX series endpoints are next-generation endpoints that deliver powerful, high-quality communications and collaboration for a variety of office environments. The Cisco DX series endpoints provide native support for HD video up to 1080p30 using the video codec H.264. They also support the annex codec H.264 AVC for HD video at even less bandwidth. Many features are supported on these endpoints, such as access to cloud services, IM, and presence with Cisco Jabber and support for EM. The three main capabilities of DX series endpoints are registration to the Cisco Unified CM for audio and video call admission and control, an Android-based applications feature that increases productivity in the workplace, and an administrative function that allows complete control over what features on the Cisco DX series endpoints are available for users to access. In addition, the Cisco DX series endpoints have a built-in function that allows Cisco Intelligent Proximity for Mobile Voice to be leveraged through Bluetooth technology, so contacts and call history can be shared between your smartphone and the endpoint, and mobile phone calls can be picked up, mid-call, from the Cisco DX series endpoints.

Cisco DX series endpoints register exclusively with the Cisco Unified CM. The process for registering these endpoints is the same as other devices within the Cisco unified communications and collaboration portfolio. This simplifies the process by not having extra steps in the process, and it simplifies the troubleshooting process should problems be encountered. Certain settings must be configured on the Cisco Unified CM before the endpoint can register. Best practice is to configure the Cisco Unified CM first, and then set up Option 150 and let DHCP deliver the TFTP addresses to the Cisco DX series endpoints. This “behind the curtain” approach makes setup of the Cisco DX series endpoints as simple as cabling up and powering on the endpoint for the endpoint to register with the Cisco Unified CM.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 9-4 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 9-4 Key Topics for Chapter 9

Key Topic Element	Description	Page Number
Paragraph	Identify different features available on the Cisco DX series endpoints.	200
Paragraph	Identify the three main capabilities on the Cisco DX series endpoints.	201
Paragraph	Understand the different protocols Cisco DX series endpoints use to communicate with the Cisco Unified CM.	204
Step list	Understand the process on how to reset Cisco DX series endpoints using the application's Setting menu.	204
Step list	Understand the process on how to reset Cisco DX series endpoints using the key-press sequence.	204
Paragraph	Know which Cisco DX series endpoints support PoE.	205
Paragraph	Understand how Cisco DX series endpoints use the Intelligent Proximity for Mobile Voice feature.	206
Paragraph	Understand when its necessary and how to set up a PIN or password for the Cisco DX series endpoints.	206
Paragraph	Understand the importance of how the Cisco Unified CM uses the MAC address of endpoints to identify them.	207
Table 9-3	Know the required settings that must be configured on the Cisco Unified CM before Cisco DX series endpoints can register.	210

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

CDP, LLDP-MED, PoE, DN, MAC address, device pool, phone button template, calling search space (CSS), owner, owner user ID, phone load name, allow control of device from CTI, device security profile, SIP profile, Secure Shell user, Secure Shell password, web access, SSH access

This page intentionally left blank

This chapter covers the following topics:

- **Cisco TelePresence TC Software-based Endpoint Setup:** This section examines five different options that you can use to interface with TC software-based endpoints.
- **Registering a Cisco TelePresence TC Software-Based Endpoint with a Cisco Unified CM:** This section shows how to configure a TC software-based endpoint with the Cisco Unified CM using SIP.
- **Registering a Cisco TelePresence TC Software-Based Endpoint with a Cisco VCS:** This section shows how to configure a TC software-based endpoint with the Cisco VCS using SIP and H.323.
- **Calibrating a Cisco TelePresence TC Software-Based Endpoint:** This section explains different options available on a TC software-based endpoint that you can use to calibrate audio and video and phonebooks.
- **Cisco TelePresence TC Software-Based Endpoint Call Scenarios:** This section explains how to configure call settings, place and receive calls, how to share content, and how to perform near- and far-end camera control.
- **Cisco TelePresence TC Software-Based Endpoint User Accounts:** This section covers two of the different user accounts available on the TC software-based endpoints and how to secure an endpoint for user operation and calls within a network.

Configuring Cisco TelePresence TC Software-Based Endpoints

When TANDBERG acquired a company called Codian, the engineers at Codian were developing an endpoint. After the acquisition, TANDBERG finished the development project and named the software for the endpoints TC, for TANDBERG Codian. All TC software-based endpoints can be configured the same way, and the interfaces are the same, making it easy for an administrator to deploy different models of TC software-based endpoints.

This chapter discusses a beginning-to-end process that shows how to configure the TC endpoint for both a Cisco Unified Communications Manager (CM) and a Cisco Video Communications Server (VCS). The discussion also covers how to calibrate an endpoint to the room environment and how to set up and support user accounts and control basic calling features.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 10-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 10-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Overview	1
Cisco TelePresence TC Software-Based Endpoint Setup	2–3
Registering a Cisco TelePresence TC Software-Based Endpoint with a Cisco Unified CM	4
Calibrating a Cisco TelePresence TC Software-Based Endpoint	5–6
Cisco TelePresence TC Software-Based Endpoint Call Scenarios	7–8
Cisco TelePresence TC Software-Based Endpoint User Accounts	9–10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. In a SIP call using Early Offer, what information is sent with the initial Invite message?
   a. SIP
   b. SDP
   c. H.225
   d. H.245
2. Which of the following is not a method of interfacing with TC software-based endpoint?
   a. Web interface
   b. Touch 8
   c. Touch 12
   d. CLI through serial interface
3. Which of the following statements is true about how to set up Intelligent Proximity for Content Sharing on a TC software-based endpoint?
   a. Intelligent Proximity for Content Sharing cannot be used on SX10 endpoints.
   b. Nothing needs to be done on the endpoint to use Intelligent Proximity for Content Sharing.
   c. Intelligent Proximity for Content Sharing requires a Bluetooth connection to the endpoint.
   d. Intelligent Proximity for Content Sharing must be turned on at the endpoint.
4. How does the Cisco Unified CM identify a TC software-based endpoint when it tries to register?
   a. By the IP address of the TC software-based endpoint
   b. By the MAC address of the TC software-based endpoint
   c. By the serial number of the TC software-based endpoint
   d. By the RRQ of the TC software-based endpoint
5. Which of the following is a phonebook that TC software-based endpoints can receive from the Cisco TMS?
   a. Enterprise phonebook when the TC software-based endpoint is registered with the Cisco Unified CM
   b. Corporate phonebook when the TC software-based endpoint is registered with the Cisco VCS

c. Corporate phonebook when the TC software-based endpoint is registered with the Cisco Unified CM

d. Local phonebook no matter where the TC software-based endpoint is registered

6. What type of encryption can TC software-based endpoints use when registered to the Cisco Unified CM?

a. DES 56-bit encryption

b. AES 128-bit encryption

c. SRTP and TLS only

d. All encryption types

7. Which menu would an administrator use to configure auto-answer on a TC software-based endpoint using the web interface?

a. **Configuration > System Configuration > Configuration**

b. **Configuration > System Configuration > Auto Answer**

c. **Configuration > System Configuration > Network Settings**

d. **Configuration > System Configuration > Experimental**

8. What does FECC allow users to do on a TC software-based endpoint?

a. Share content during a call

b. View content during a call

c. PTZ the camera of a connected endpoint during a call

d. Used for Ethernet call connections, allowing calls to connect over an IP network

9. Which of the following statements is true about a factory reset on a TC software-based endpoint?

a. Factory resets only wipe out configuration settings, not upgraded image files.

b. Factory resets only wipe out configuration settings, not upgraded image files or IP settings.

c. Factory resets wipe out configuration settings and upgraded image files.

d. Factory resets cannot be performed on TC software-based endpoints.

10. Which of the following user accounts exist on TC software-based endpoints by default?

a. Admin and helpdesk

b. Admin and root

c. Admin only

d. Root only

Foundation Topics

Cisco TelePresence TC Software-Based Endpoint Overview

Cisco TC software-based endpoints can register with a Cisco Unified CM using Session Initiation Protocol (SIP), or they can register with the Cisco VCS using SIP or H.323. To better understand the Cisco TC software-based endpoints, an understanding of how the endpoints communicate with both call control servers is needed. Whether the Cisco Unified CM or the VCS is being used for communication using SIP, both call control servers are acting as a SIP server. The SIP server is often referred to as the SIP proxy or the SIP registrar, although these are actually functions of the SIP server. If the endpoint is communicating to the VCS using H.323, the VCS is acting as an H.323 gatekeeper. These terms are important for later discussions.

Configuring a TC Endpoint to Register with a Cisco Unified CM

If an administrator is configuring a TC endpoint to register with a Cisco Unified CM, the fist step is to cable up the endpoint and turn it on. How the endpoint is cabled up will depend on the type of endpoint being used. You may want to review Chapter 7, "Cisco TelePresence Endpoint Characteristics," where these different options are discussed in length. After the endpoint has booted and loaded its locally stored image file, it can be configured to register with the Cisco Unified CM. TC endpoints can use Cisco Discovery Protocol (CDP) for VLAN discovery, but this option is disabled on the endpoint by default. When the unit is configured to register with the Cisco Unified CM VLAN, discovery is enabled. If an administrator wants to use VLAN discovery in a VCS environment, this setting must be enabled manually.

When VLAN discovery is complete, the endpoint sends a DHCP Discovery message to the DHCP server. Similar to a UC environment, Option 150 can be made available for the TFTP server address to be discovered at the same time; however, the **DHCP RequestTFTPServerAddress** setting on a TC endpoint must be enabled for TFTP discovery to work. For the time it takes to turn this setting on, the External Manager settings could be configured, so it may prove most prudent just to configure the External Manager settings manually.

Now that the endpoint has appropriate IP address information and the TFTP server address, it can send a TFTP Get message to the TFTP server. The communication the endpoints send to the TFTP server contains their MAC addresses because that is what the Cisco Unified CM uses to identify the endpoint. Similar to UC environments, the first element the endpoint tries to download is a certificate trust list (CTL) file. The CTL file contains a set of certificates and is used only when Cisco Unified CM cluster security has been enabled. Next, the endpoints try to download their own configuration files. After the configuration file has been downloaded, the endpoints verify that they are running the requested load or firmware version. TC endpoints will not try to download upgrade firmware files. Although this is Cisco's intent for future versions, as of 10.x on the Cisco Unified CM the TC endpoint only validates if the version it is running is a supported version.

The final step in the process is for the endpoints to register with the Cisco Unified CM. The endpoints send their IP address with their alias information to the Cisco Unified CM and request registration. The Cisco Unified CM responds with a SIP 200 OK message. Now the registration process is complete.

Registering a TC Software-Based Endpoint with the Cisco VCS Using SIP

Registering a TC software-based endpoint with the Cisco VCS using SIP is different in many ways. In a UC environment, configuration settings are created on the Cisco Unified CM and then pushed to the endpoint when requested. In a VCS environment, configuration settings are manually entered on the endpoint. Also, VLAN discovery is not necessary when registering with the VCS. The endpoint does not need to be aware of the VLAN it is a part of to use quality of service (QoS), nor does the VCS takes part in implementing QoS. So, after the endpoint has booted and performed DHCP discovery, it tries to register with the VCS based on the information manually configured on the endpoint. The endpoints send their IP address with alias information to the Cisco VCS and request registration. The Cisco VCS should respond with a SIP 200 OK message. Figure 10-1 illustrates the generic registration process with a SIP server.

Key Topic

Figure 10-1 *Endpoint Registration with a SIP Server*

When endpoints are registering with a SIP server, the server is acting in the capacity of a SIP registrar. The SIP registrar is responsible for creating a table mapping the IP address of an endpoint to the alias being used. SIP servers typically use URI dialing in the form of Host@FQDN (fully qualified domain name). Therefore, the domain must be configured on the SIP server before endpoints are allowed to register. The Cisco Unified CM uses directory numbers (DNs), but they register as DN@CUCM IP address. URI addresses can be added to a DN if administrators want users to leverage URI dialing within their environments. On a VCS, the FQDN is essential for SIP registration where endpoints register with full URIs. Also, it is important to note that SIP uses UDP port 5060 for registration on both the Cisco Unified CM and the Cisco VCS.

Registering a TC Software-Based Endpoint with the Cisco VCS Using H.323

The registration process for H.323 is a lot chattier. Because the Cisco Unified CM does not support H.323 natively, a VCS must be used for gatekeeper registration in an H.323 environment. The process begins in a similar fashion to SIP registration with a VCS. After the endpoint has booted, H.323 settings must be configured on the endpoint manually. Then the endpoint tries to register with the gatekeeper. How that gatekeeper is discovered depends on how *discovery mode* is configured. If discovery mode is configured as

automatic, the endpoint sends out a broadcast message to the switch requesting a gatekeeper to register with. This broadcast message is called a Gatekeeper Request (GRQ) and uses UDP port 1718. The first gatekeeper to respond with a Gatekeeper Confirm (GCF) will be the gatekeeper the endpoint will try to register with. This might not be the gatekeeper the administrator intended to register with, however. Therefore, best practice suggests that discovery mode be configured as *manual*. In manual mode, a gatekeeper address must be configured on the endpoint. This will be the only address the endpoint will try to register with.

After the gatekeeper address has been discovered or manually entered on the endpoint, the next message the endpoint sends is a Registration Request (RRQ) using UDP port 1719. The gatekeeper responds with a Request In Progress (RIP) message because there are security settings on the VCS that can prevent an endpoint from registering. After these settings have been checked, provided there are no limitations, the gatekeeper sends a Registration Confirm (RCF), and the endpoint is now registered. If an issue prevents the endpoint from registering, it receives a Registration Reject (RRJ) message from the gatekeeper. Figure 10-2 illustrates how the H.323 registration process operates with a Cisco VCS.

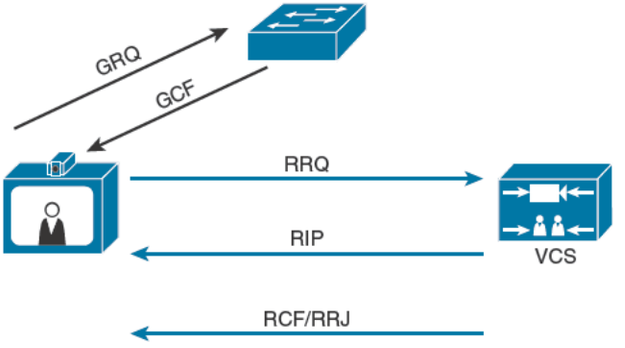


Figure 10-2 *H.323 Registration Process with a Cisco VCS*

Once an endpoint is registered, whether using SIP or H.323, a different process is used for call processing. First, the SIP call process is examined.

Call Processing with SIP

Both the Cisco Unified CM and the Cisco VCS process SIP calls in a similar fashion. Both call control servers have call admission control (CAC) elements that can be leveraged, although what these elements are and how they are leverage mark the differences between each call control server. CAC goes beyond the scope of this book, so the focus here is on basic elements of a SIP call. A SIP call can be processed in two ways: Early Offer and Delayed Offer. The differences between these two methods have to do with when Session Description Protocol (SDP) is sent. SDP is the mechanism SIP uses to exchange codec capabilities and identify the UDP ports needed for Real-time Transport Protocol (RTP) media. Only Early Offer is described in the following example.

When a source endpoint dials the destination alias using SIP, an *Invite* message is sent to the SIP server with its SDP information. In this case, the SIP proxy function examines the table created by the SIP registrar to determine the destination endpoint's IP address by

the alias dialed. The SIP server will then proxy the Invite message with the SDP packets to the destination endpoint and respond to the source endpoint with a *Trying* message. The Trying message contains the destination endpoint's IP information. Once the Trying message is received, the source endpoint now possesses the source and destination IP addresses.

When the destination endpoint receives the Invite message, that endpoint now has the source and destination IP address information. It then responds with two messages. The first message is the Ringing message. This Ringing communication tells the destination endpoint to ring and sends a ring-back tone to the source endpoint. Once the user of the destination endpoint answers the call, an OK message is sent. The OK message contains call connection status, acknowledgment that SDP information has been received, and the destination endpoint's SDP communication. Because the destination endpoint now knows the ports the source endpoint specified for the media communication, those ports are opened, and the destination endpoint can now receive audio and video media over those UDP ports.

When the source endpoint receives the OK message from the destination endpoint, the UDP ports specified from that communication are opened, so audio and video media can be received from the destination endpoint. An acknowledgment is sent to the destination endpoint, and the call is now set up. Figure 10-3 illustrates the call setup process for SIP communication.

Key Topic

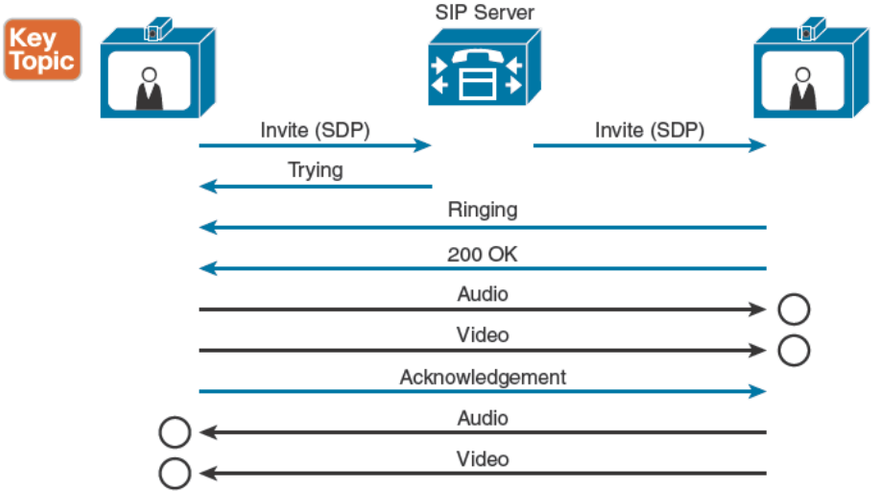


Figure 10-3 *SIP Call Setup Process*

Call Processing with H.323

The H.323 call process is a lot chattier than the SIP call process. Because the Cisco VCS is the only H.323 gatekeeper Cisco has, this explanation references the VCS. When a device, whether it is an endpoint, multipoint control unit (MCU), or a gateway, registers with a gatekeeper, that device is completely subservient to the gatekeeper. Therefore, it must have permission before it can do anything. So, if an endpoint wants to place a call to another endpoint registered to the same VCS, the source endpoint must first send an Admission Request (ARQ) to the VCS to request permission to call. This message is sent when the

source endpoint dials the destination alias. When the VCS receives the ARQ message, it responds with a Request In Process (RIP) message. This is when the VCS reviews all CAC settings that have been configured and tries to locate the destination alias. If there is some CAC in place that prohibits the call from continuing, the VCS sends an Admission Reject (ARJ) to the source endpoint, and the call attempt ends. If there is no CAC in place that prohibits the call from continuing, the VCS sends an Admission Confirm (ACF) to the source endpoint. This ACF contains the destination endpoint's IP address. Using that IP, the source endpoint sends an H.225 Call Setup message. This message is sent using the Q.931 protocol from the ITU H.320 umbrella standard for circuit-switched communication. (This was a carryover protocol when the ITU developed the H.323 umbrella standard for packet-switched communication.)

When the destination endpoint receives the Call Setup message, it sends the VCS its own ARQ message requesting permission to answer the call. The VCS responds with a RIP message, then an ACF. (Because the two endpoints in this scenario are registered to the same VCS, and there was no CAC prohibiting the call during the first ARQ message, there will be no prohibitions during this second ARQ. If the destination endpoint were registered to a different gatekeeper, there could be cause for CAC to prohibit the destination endpoint from answering the incoming call.) When the ACF is received, the destination endpoint sends two messages to the source endpoint. The first message sent is an H.225 Alerting message using the same Q.931 protocol mentioned before. This Alerting message tells the destination endpoint to ring and sends a ring-back tone to the source endpoint. When the user of the destination endpoint answers the call, an H.225 Connect message is sent using the Q.931 protocol.

Most TCP communication uses a three-way handshake (SYN, ACK, SYN/ACK) to establish communication before important packets are sent. In an H.323 call, the call setup process establishes that same open line of communication needed before critical capabilities and UDP port allocations are sent between the two endpoints. The standard used to send this information is H.245. Because this information is sent over TCP, acknowledgments are also sent to confirm receipt of the information being exchanged. The first sets of packets exchanged between the two endpoints are the capabilities exchange. This identifies what audio and video codecs each endpoint supports, in addition to any other capabilities that exist, like far-end camera control (FECC) or content sharing. Next is the master/responder negotiation. (The ITU labels this communication as master/slave negotiation, but it has become common to refer to it as responder instead of slave.) A master must be decided between the two endpoints, and the master will decide what codec is to be used for each capability and what UDP ports each endpoint will use to transmit the packets over. Once the master is decided, that endpoint sends the codec selection and port allocation for itself and the destination endpoint to the destination endpoint. When all the port are open, two-way communication can take place. Figure 10-4 illustrates the H.323 call setup process.

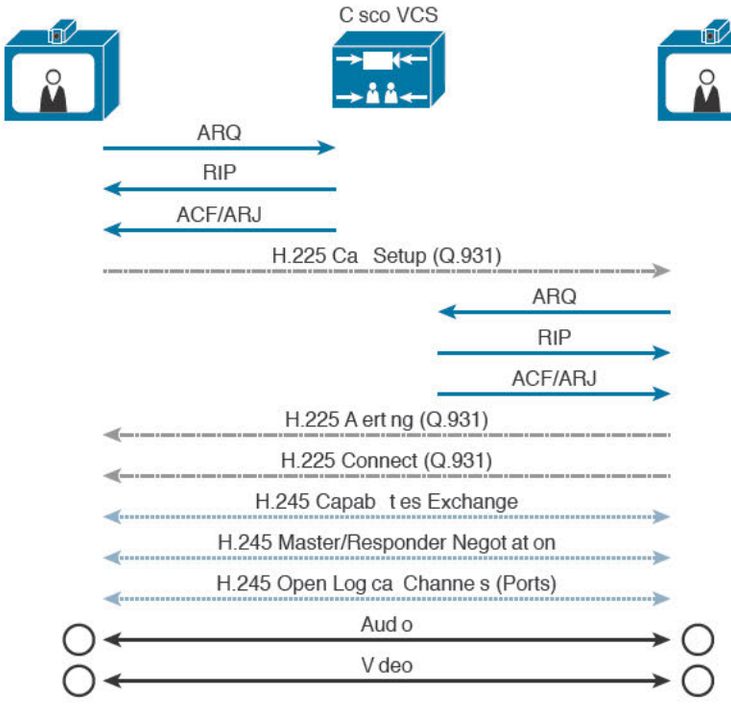


Figure 10-4 *H.323 Call Setup Process*

Now you should understand how Cisco TC software-based endpoints register with a Cisco Unified CM using SIP, and with the Cisco VCS using SIP and H.323. You also learned how H.323 and SIP calls are processed. Before an endpoint can be configured for registration or calls, it is important to understand how an administrator or end user can interface with an endpoint.

Cisco TelePresence TC Software-Based Endpoint Setup

Key Topic

A user can interact with the TC software-based endpoints in five different ways:

- Using the onscreen-display (OSD) with the remote control
- Using the web interface via HTTP or HTTPS
- Using the command-line interface (CLI) via Telnet or Secure Shell (SSH)
- Using the Cisco Touch 8 or Touch 10
- Using the new Cisco Intelligent Proximity for Content Sharing

Using the Onscreen Display with the Remote Control

The remote control used with all TC endpoints, except for the SX10, is the TRC5 remote. Using this, remote administrators and users can perform most all the functions they need from configuring endpoints to placing calls. However, the SX10 uses a TRC6 remote, which can only be used by users to place calls. All other configuration settings must be done on the SX10 endpoints from either the web interface or the CLI.

Note The SX10 does have a Setup Wizard that can be used to provision the endpoint during the first time it is booted. Device settings must be provisioned from the TFTP server for Cisco Unified CM registration or from TMS (TelePresence Management Suite) for VCS registration.

Figure 10-5 illustrates the button layout of the TRC5 remote control.

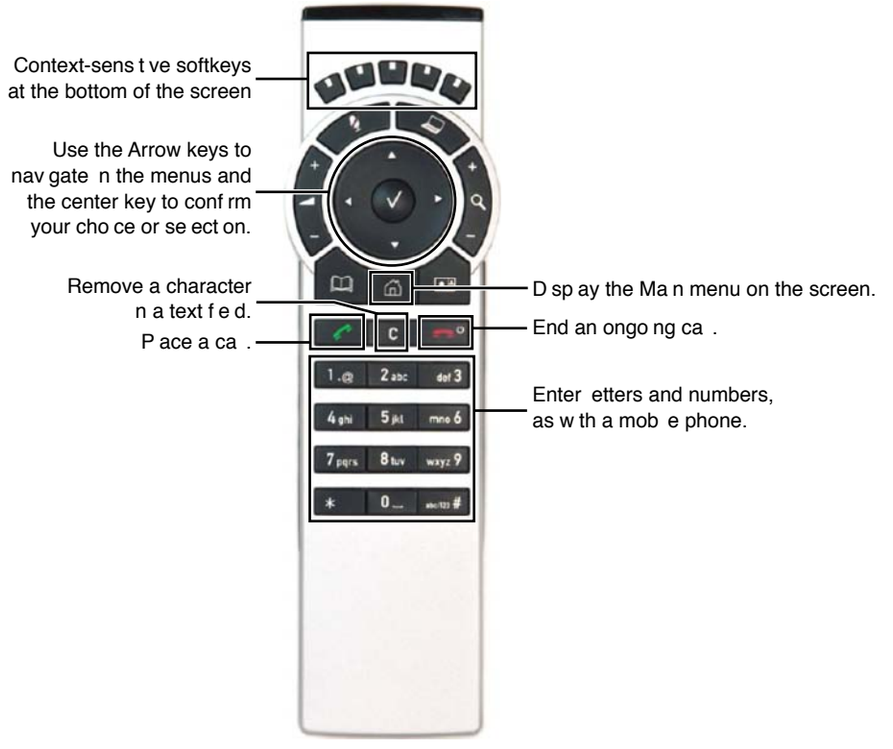


Figure 10-5 *TRC5 Remote Control*

As Figure 10-5 illustrates, five soft keys are located at the top of the remote control. These keys correspond with soft key options that display across the bottom of the display. Different options are made available depending of what the endpoint is doing. For example, if a user is in a call, there is a soft key option for FECC. If an administrator is configuring a

setting on the endpoint, there is a soft key option to toggle between numbers and letters. Some soft key options are programmable as well. Below the soft keys in the center of the remote are arrow keys with a checkmark button in the center of them. These arrow keys can be used to navigate menus and to pan and tilt the camera, whether near-end or far-end camera control is being used. The checkmark button is like an Enter key used to make selections. The Zoom button for camera control is located to the right of the arrow keys, and the Volume button is located to the left. Just above the arrow keys are two buttons. The left one is for muting the microphone, and the right one is for sharing content if a device, like a computer, is connected to the endpoint. Below the arrow buttons are three more button options. The left button bring up the phonebooks on the endpoint. The center button is a home button. This displays the main menu options no matter where you have navigated within the menus, or even if there are no menus displayed. The right button is used to bring up the self-view of the camera connected to the endpoint. It can also be used to change the layout if the multisite option is being used. Above the number keypad is the Call Answer and Call Disconnect button. Between them is a C button. This is a Clear, or Backspace, button. It also takes you to the previous menu set when navigating menus using the remote control.

Pressing the Home button or the Checkmark button will bring up the first level of menus. Any menu option that has a black arrow beside it means that selecting it will offer another level of menu options. From the main level menus, navigating to **Settings > Administrator Settings > Advanced Configuration** will take administrators to the menus used to configure and calibrate an endpoint. Figure 10-6 illustrates how these menus will appear.

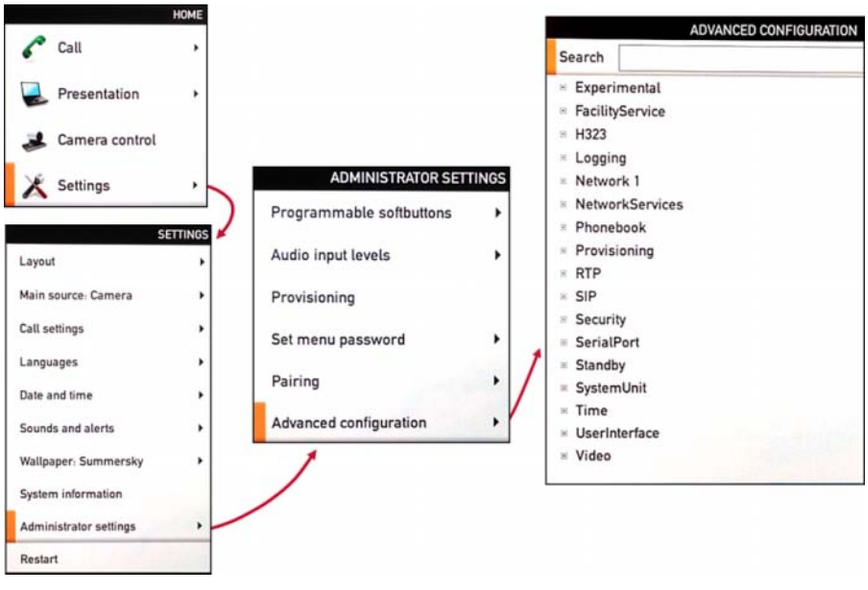


Figure 10-6 *OSD Menus Using the Cisco TRC5 Remote Control*

Using the Web Interface via HTTP or HTTPS

The web interface of TC software-based endpoints is a great way to perform more advance functions on the endpoint for administrators who are not familiar with the CLI. The browsers that can be used are mostly all encompassing. Internet Explorer is the most problematic. Firefox and Chrome seem to work the best. Distinguished from the OSD, the main menus of the web interface are horizontally listed across the top of the page. Scrolling over a menu will display the submenu options available. The main configuration and calibration menus can be access by navigating to **Configuration > System Configuration**. These menu options are listed exactly the same as they are listed using the OSD. Figure 10-7 illustrates how the web interface menus should appear as of Version TC7.x.

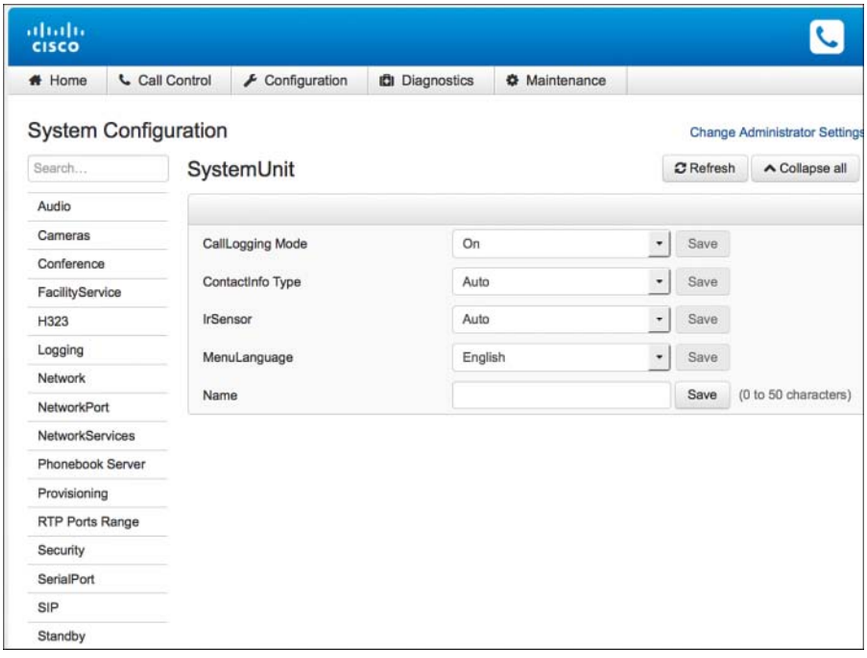


Figure 10-7 *Web Interface of a TC7.x Endpoint*

Using the Command-Line Interface via Telnet or SSH

For administrators who are already familiar with the menus on TC software-based endpoints, the CLI is a great option for interfacing with them. The CLI can be accessed using either Telnet, SSH, or the RS232 serial port available on most TC software-based endpoints. If the serial interface is used, it is important to note that the bit rate is preset on the endpoint at 38400. This setting can be changed, but it is not recommended. There are more options that an administrator can use with the CLI than any other way someone might interface with these endpoints. TC endpoints are built on a Linux platform, and the commands are relatively easy to use. The **Help** command or the **?** command will list all available commands or subcommands, guiding administrators to the exact code line needed. There are three main commands used on TC endpoints: **xCommand**, **xConfiguration**, and **xStatus**. If an administrator wants to tell the endpoint to do something, like place a call or reboot, the **xCommand**

code lines are used. If an administrator wants to verify the status of a call, check network settings, or view the registration status for H.323/SIP, or some other status, the **xStatus** code line is used. If an administrator wants to configure a setting on the endpoint, the **xConfiguration** code lines are used. For example, if an administrator wants to identify a system name for an endpoint, the command used is **xConfiguration SystemUnit Name:** <*system name*>. The code used with **xConfiguration** maps exactly to the menu structure of the web interface and the OSD. Figure 10-8 lists the commands under **xConfiguration** using the CLI.

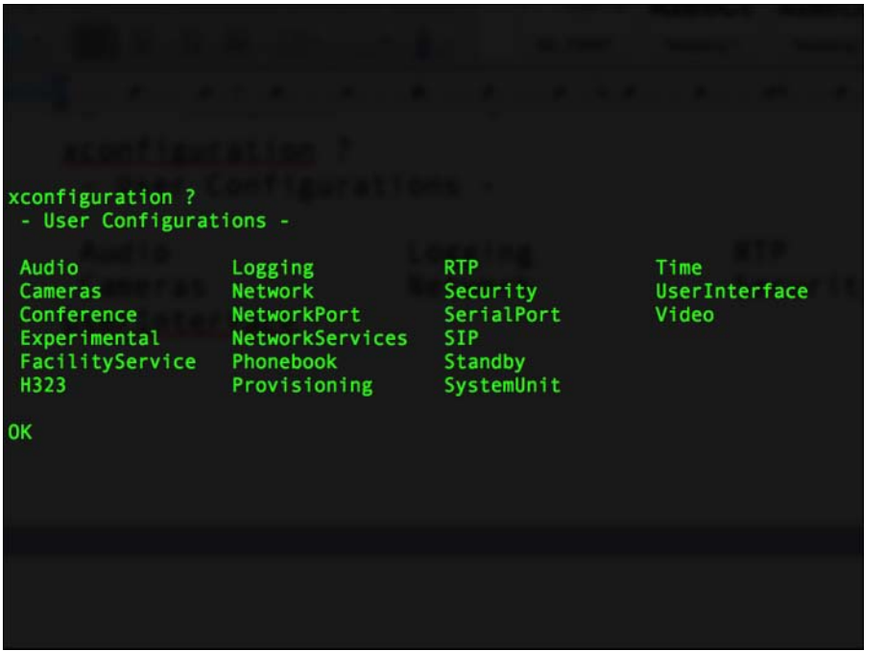


Figure 10-8 *xConfiguration Commands Using CLI*

10

Using the Cisco Touch 8 or Touch 10

The forth way users can interact with TC software-based endpoints is by using the Cisco Touch control pad. As mentioned in Chapter 7, the Cisco Touch 10 is used only with MX200G2, MX300G2, MX700, and MX800 endpoints. The EX60 and EX90 come with a Touch 8. The TRC5 remote can be used with these endpoints, but they default using the Touch 8. Also, the Touch 8 used with the EX series endpoints can only be used with those endpoints. However, another Touch 8 option is available for all other TC software-based endpoints except for the SX10. Touch control pads are intended as an easier option for users to interact with TC endpoints. Users can use the Touch control pad to launch calls, end calls, mute microphones, view and select participants from directories, share content, and view statistic information about a call. However, most administrative options are not included with the Touch control pads. All Cisco Touch control pads do require a physical connection to the endpoints they are controlling. For endpoints that have a dual network interface card (NIC) port available, the Touch can be plugged into that available port. If the

distance from the Touch to the endpoint is greater than 7.5 meters (about 25 feet), it can be connected to a Power over Ethernet (PoE) switch port or through a power injector. This extends the reach of the Touch an additional 5 meters (16 feet).

Key Topic

Using Intelligent Proximity for Content Sharing

Intelligent Proximity for Content Sharing is the fifth way a user can interface with an endpoint. The function of Intelligent Proximity has already been explained in Chapter 7. For Intelligent Proximity to be used on a TC software-based endpoint, the setting must first be turned on at the endpoint. From the web interface, navigate to the System Configuration menus and type **byod** in the search bar. Two settings will be displayed. CashedSnapshots will be preset to 10 and can be changed up to 20. If the far end is sharing content you are viewing using Intelligent Proximity, this number identifies how many slides you can go back and view even though the presenter has moved passed them. The other setting displayed is the Mode. This setting is defaulted as off and must be set to on before Intelligent Proximity can be used with this endpoint. Because Intelligent Proximity uses a high-frequency tone to initially sync the device with the endpoint, the volume for this tone can be set as well. To adjust this volume, type **AudioPair** in the search bar. It defaults at a setting of 70 and can be changed up to 100. Next, the Intelligent Proximity application must be installed on your device. See Chapter 7 for information about where it can be retrieved for different devices. After the application has been installed, make sure that your device is connected to the same network, open the application, and Intelligent Proximity will automatically connect. Figure 10-9 shows what Intelligent Proximity looks like on an iPhone when it searches for the endpoint and once it connects.

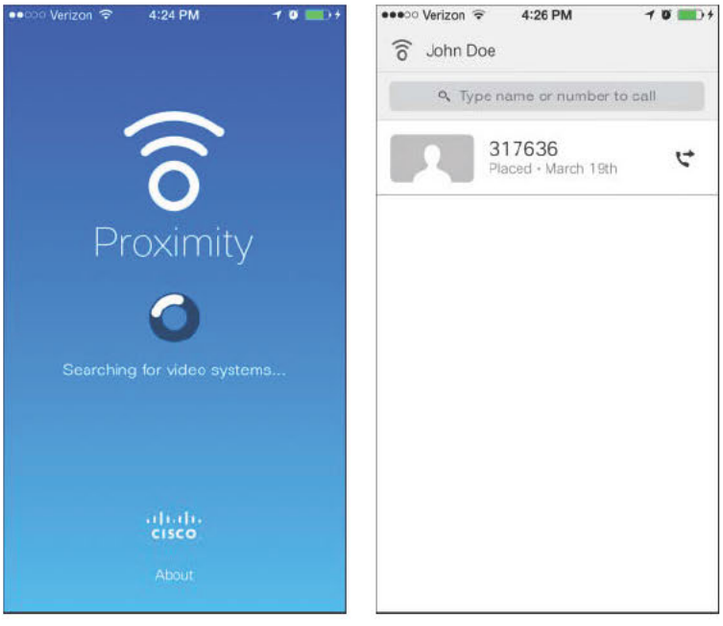


Figure 10-9 *Intelligent Proximity on an iPhone*

Registering a Cisco TC Software-Based Endpoint with a Cisco Unified CM

The web interface, the OSD with remote control, or the CLI can be used to register a TC software-based endpoint. TC endpoints can register with either the Cisco Unified CM using SIP or to the Cisco VCS using H.323/SIP. This section shows how to use the web interface to register a TC endpoint to the Cisco Unified CM. Unlike UC endpoints, including DX series and CTS series, TC software-based endpoints do not default to use Option 150, nor do they default to register with the Cisco Unified CM. Therefore, these settings must be configured on the endpoint if you want to use them. The location in the configuration settings to set the Cisco Unified CM as the call control server is the same location the address of the TFTP server is entered. Therefore, it does not make sense to use Option 150 on a TC endpoint, because you would have to navigate to a different menu altogether on the endpoint, just to turn it on. The following steps describe how to configure a TC endpoint when Option 150 is not being used. Also, the endpoint will not register with the Cisco Unified CM unless it knows the endpoint by its MAC address.

Key Topic

After you have logged in to the endpoint through the web interface, navigate to **Configuration > System Configuration** and click the **Provisioning** menu located in the left column. Change the **Provisioning Mode** to **CUCM** and click **Save**. Just below this setting, enter the address of the TFTP server in the External Manager Address field and click **Save**. The endpoint should register with the Cisco Unified CM after about 1 minute. To verify the endpoint has registered, click the **Home** menu across the top of the page. Under the SIP heading, the status should show as registered, the proxy address should be the CUCM node that supports registration, and the URI should be the directory number (DN) assigned to the endpoint.

Because TC endpoints cannot register with the Cisco Unified CM using H.323, this mode can be turned off. To do so, navigate to **Configuration > System Configuration**. Click the **Network Services** menu, turn off **H.323 Mode**, and click **Save**.

Registering a Cisco TC Software-Based Endpoint with a Cisco VCS

As mentioned in the previous section, TC software-based endpoints can register with the Cisco VCS using either H.323 or SIP. The provisioning mode used to set the Cisco Unified CM as the call control server does not need to be configured when registering a TC endpoint to the VCS. The default setting for the provisioning mode is TMS, and there is a VCS setting as well. However, because the VCS does not provision endpoints, this setting has no relevance when registering them with a VCS. In the previous section, H.323 mode was turned off. The default for this setting is on. Assuming that this is an install of a new endpoint, there is little need to check that this setting is turned on. If this is an endpoint that has already been used in a production environment, you may want to verify the H.323 mode.

To configure H.323 on a TC software-based endpoint, navigate to **Configuration > System Configuration**. Click the **H.323** menu in the left column. NAT mode is off by default and should not be turned on. Under the Profile 1 settings, the first setting you will see is the Call Setup Mode. This setting can be configured as Gatekeeper or Direct, and Gatekeeper is the default setting. In direct mode, the endpoint will not register with any gatekeeper. It can still place calls, but only by the IP address of the destination endpoint. No RAS (Registration, Admission, Status) messages will be sent from or to this endpoint because it does not require a gatekeeper. Leave this setting as **Gatekeeper**.

The next significant settings under Profile 1 are the gatekeeper settings. They are address and discovery. Address is the address of the gatekeeper you want to register the endpoint with; in this case, it is the VCS. Discovery determines how the endpoint will locate a gatekeeper to try to register with. Discovery mode can be configured as Manual or Auto. If configured as Auto, no gatekeeper address needs to be configured. The endpoint sends out a GRQ broadcast to locate the gatekeeper, as mentioned toward the beginning of this chapter. Manual uses the address specified in the above field. Best practice suggests leaving this setting as Manual, which is the default.

The last subheading under Profile 1 is H.323 Alias, and the options here are E.164 and ID. An E.164 alias, as defined by the ITU, is a numeric alias using digits between 0 and 9 and should be no longer than 15 digits long. Essentially, it is a phone number. The ITU ratified the parameters for E.164 alias for use with H.320 circuit-switched communications. However, E.164 aliases were carried over with the development of H.323 packet-switched communication, and the length of the alias is less significant. On TC software-based endpoints, an E.164 alias can be up to 30 digits long, although that makes for a long phone number to remember. ID represents an H.323 ID, which is the other type of alias that can be used with H.323 communications. H.323 IDs can use alphanumeric and special characters up to 49 characters long. In the past, a common use of H.323 IDs was to use a person's name. Someone could dial "John" and place a call to John's endpoint. Today, a more common use of H.323 IDs is to configure them in the form of a URI. Make no mistake: H.323 ID is not a URI. However, they can be configured in the form of a URI. In some production environments, customers configure both the E.164 alias and the H.323 ID. The E.164 alias is commonly used for internal calls, and the H.323 ID, in the form of a URI, is used for external calls. Figure 10-10 illustrates the H.323 configuration menus available on a TC software-based endpoint.

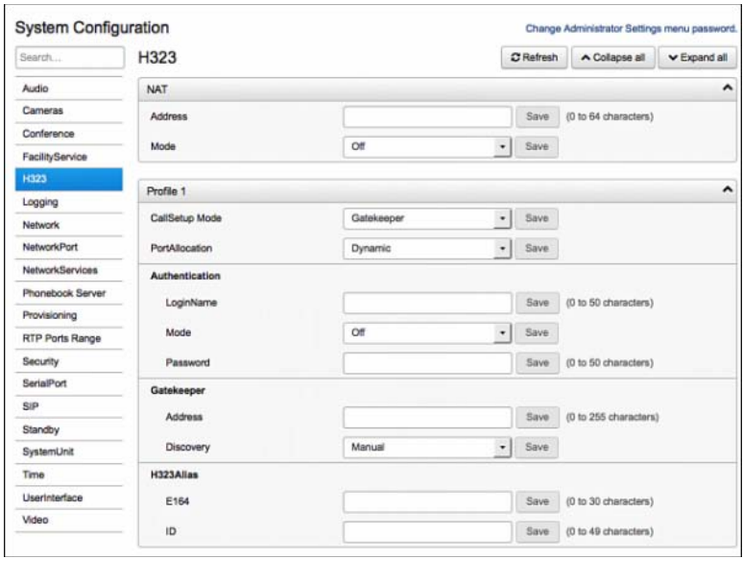


Figure 10-10 *H.323 Menus on a TC Software-Based Endpoint*

Each of the settings discussed in this section must be saved before they will take affect. Once saved, the endpoint should register with the VCS immediately. To verify the registration was successful, navigate to **Home**. Under the H.323 heading, Status should show up as Registered, Gatekeeper should be the VCS address specified in the H.323 configuration setting, Number should be the E.164 alias, and ID should be the H.323 ID.

When registering an endpoint with the VCS, an administrator can choose whether to use H.323, SIP, or both. Because the foundation for registering a TC software-based endpoint has been established for H.323, a close examination on how to register the endpoint using SIP with the VCS is needed. Again, the VCS does not provision settings to endpoints, so all SIP configuration settings need to be configured on the endpoint before it can register with the VCS. Navigate to **Configuration > System Configuration** and click the **SIP** menu in the left menu column. There are many more options available than are needed for a basic SIP registration. This section focuses on only the basic settings needed to register an endpoint with the VCS using SIP. All of these settings can be found under the Profile 1 section. The first configuration parameter listed under Profile 1 is the Default Transport. This setting can be configured as TCP, UDP, TLS, or Auto. If none of your calls should be encrypted, set it to **TCP** or **UDP**. If all calls should be encrypted, set it to **TLS**. If you want SIP calls to try encrypting first, but to connect anyway if they cannot, use **Auto**. The default setting is TCP. Another menu option is Type, which can be configured as **Standard** or **Cisco**. Standard should be used when registering to the VCS, and this is the default setting. This setting will change automatically to Cisco when registering to the Cisco Unified CM. Administrators should never need to change this setting, but it is a valuable setting of which to be aware.

Below this setting is the Display Name. This name will display on the destination endpoint's monitor when you connect. It will also be displayed when connecting through a multipoint control unit (MCU). If this setting is not configured, the URI address displays in its place. A little further down is the URI setting. This should be the URI address that users will dial when they are trying to connect to your endpoint. URI addresses must be in the form of Host@FQDN. The VCS will qualify the domain, and all SIP registrations will fail if the domain used in the URI address does not match a domain configured on the VCS. This is the marking difference between a URI and an H.323 ID. Because the H.323 ID is not actually a URI, the H.323 registration is allowed to register with a VCS regardless of what comes after the @. With SIP, however, the domain is a significant part of the alias and must qualify against domains listed on the VCS.

Some time was spent in this chapter explaining what a SIP server is and how the SIP registrar and the SIP proxy are functions of the SIP server. To point a TC software-based endpoint to the VCS for SIP registration, the Proxy 1 address must be configured. Under Proxy 1, two settings are listed: Address and Mode. Mode for SIP is the same as Mode for H.323. It can be configured as Manual or Auto and determines how the endpoint will try to locate a SIP server (VCS) to register with. Leave this setting as Manual. Under Address, configure the address of the VCS. All the previously mentioned settings need to be saved for the configurations to take place. Figure 10-11 shows how the SIP configuration menus will display on a TC software-based endpoint.

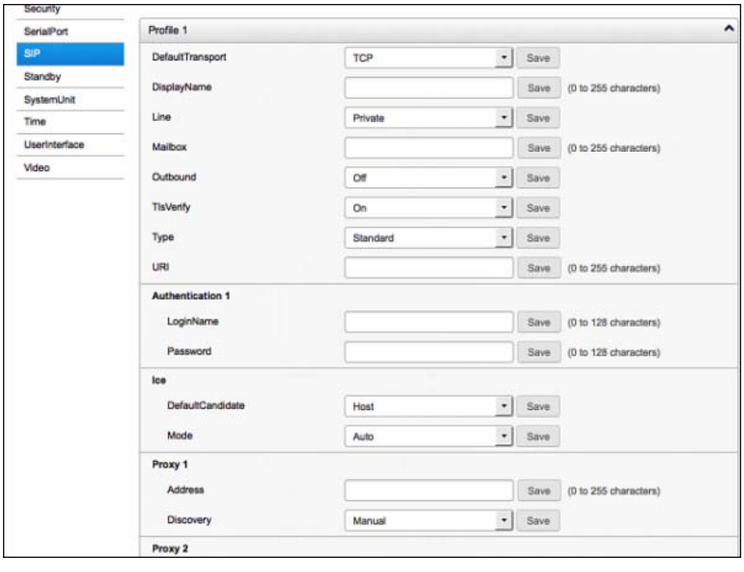


Figure 10-11 *SIP Menus on a TC Software-Based Endpoint*

To verify the endpoint has registered, click the **Home** menu across the top of the page. Under the SIP heading, Status should show as registered, Proxy should be the VCS address, and URI should be the URI address configured on the endpoint.

Calibrating a Cisco TC Software-Based Endpoint

Whether endpoints are registered with the Cisco Unified CM or with the Cisco VCS, it is important to calibrate the endpoint to the room and network environments before placing calls. This section discusses the different options available on TC software-based endpoints for calibrating audio/video input and output components, validating network settings, and subscribing to corporate directories or phonebooks. All of these settings can be configured through the web interface and the CLI. Some settings can be configured through the remote control and Cisco Touch control pads. Phonebooks can be accessed using the remote control, Touch control pad, and through Intelligent Proximity. New software versions of TC software-based endpoints can access phonebooks through the web interface as well. This section focuses on how to configure these settings, so the web interface is referenced primarily.

Calibrating Audio Input and Output Components

Audio settings can be calibrated by navigating in the web interface to **Configuration > System Configuration** menus and clicking the **Audio** menu in the left column. Audio settings are divided into four categories. The main three are Input, Output and Sound, and Alerts. The top section is untitled and contains Microphone Mute Enabled and Volume control. On some TC software-based endpoints, the HDMI port for both inputs and outputs is capable of carrying audio as well. HDMI ports that support audio will be identified within this audio section of the menus. Microphone inputs can be established as Microphone or Line in the Type menu option. Microphone is used when a single microphone is connected to each microphone port. If an external amplifier is used to connect multiple microphones, then the type for the Microphone line the amplifier is connected to should be changed to Line. An example of when an amplifier might be used is in large conference rooms. Often, A/V integrators will hang multiple microphones from the ceiling or around the conference table, exceeding the number of microphone inputs an endpoint can natively support. Both the amplifier and the TC software-based endpoint have built-in echo cancellation. If both are used at the same time, one will cancel out the other, and echo will not be filtered. Therefore, you might want to disable echo cancellation on the endpoint when external amplifiers are being used. Table 10-2 lists all the possible audio settings available on a Cisco TelePresence C90 because this endpoint has the most available input and output options within the TC software-based platform.

Key Topic

Table 10-2 C90 Audio Calibration Options

Connector	Section	Options
	Unspecified	Default Volume
	Unspecified	Microphone Mute Enabled
	Unspecified	Volume
HDMI3	Input	Level, Mode, Mute on Inactive Video, Video Input Source
HDMI4	Input	Level, Mode, Mute on Inactive Video, Video Input Source
Line 1–4 (RCA)	Input	Channel, Level, Loop Suppression, Mode, Equalizer ID and Mode, Mute on Inactive Video, Video Input Source

Connector	Section	Options
Microphone 1–8	Input	Level, Mode, Type, Echo Control De-Reverberation Mode and Noise Reduction, Equalizer ID and Mode, Mute on Inactive Video, Video Input Source
HDMI1	Output	Level, Mode
HDMI3	Output	Level, Mode
Line 1–4 (RCA)	Output	Channel, Level, Mode, Type, Equalizer ID and Mode
Key Tones Mode	Sounds and Alerts	On, Off
Ring Tone	Sounds and Alerts	Ascent, Calculation, Delight, Evolve, Mellow, Mischief, Playful, Reflections, Ringer, Ripples, Sunrise, Vibes
Ring Volume	Sounds and Alerts	0–100

Calibrating Video Input and Output Components

Video settings can be calibrated by navigating in the web interface to **Configuration > System Configuration** menus and clicking the **Video** menu in the left column. Video settings are divided into eight categories:

- An undefined basic settings category located at the top of the page
- CamCtrlPip CallSetup
- Input
- Layout
- OSD
- Output
- PIP
- SelfviewDefault

The undefined basic settings include the following:

- **AllowWebSnapshots** that allow for a snapshot of participants during a call to be viewed from the web interface.
- **DefaultPresentationSource** determines which video input port will be used for presentation sharing, if users try to share content during a call.
- **MainVideoSource** determines which camera will be used first if multiple cameras are daisy-chained together on an endpoint. Camera selection can be changed at any point during a call using the remote control or the Touch controller.
- **Monitors** allow an administrator to select how many monitors will be used during installation and what purpose each monitor will perform:
  - For example, one of the options is Dual Presentation Only, which means that the second monitor will be used only to display presentation content, whether it comes from

or is sent to that particular endpoint. The use of multiple monitors requires an option key before it can be used. That option key comes standard on some TC software-based endpoints and is a purchasable item on others. Check with your Cisco Partner to identify which endpoints the option key comes standard on.

- Selfview allows users to see their own camera view in a picture-in-picture (PIP) on their monitor.
- SelfviewPosition determines where on the monitor the self-view PIP will be displayed.
- Wallpaper is the background view users will see on their monitor when not in a call. You can choose from a stock image Cisco has already loaded on the endpoint, or you can upload an image to the endpoint for use.

Some other significant settings that can be configured for video calibration include the following:

- Under OSD, Output determines the main OSD to be used. This monitor is the only one that will display the menus if the remote control is being used. It is also the main monitor that video will be displayed on in a Point-to-Point call.
- Just below this setting is TodaysBookings. This settings will display all conferences this endpoint has been scheduled to join in a small window located in the top-right corner of the monitor.
- Under Output, there is an OverscanLevel setting for each output port that can be used to adjust the display resolution settings in case the displayed screen is outside the monitors borders.
- Below this setting is a resolution setting that can also be used to adjust the resolution.

Many more settings can be calibrated from this menu. Table 10-3 lists all the possible video settings available on a Cisco TelePresence C90 because this endpoint has the most available input and output options within the TC software-based platform.

Key Topic

Table 10-3 C90 Video Calibration Options

Menu	Section	Options
Allow Web Snapshots	Unspecified	On, Off (Can only be configured from the remote control or CLI with a serial connection)
Default Presentation Source	Unspecified	1–5
Main Video Source	Unspecified	1–5
Monitors	Unspecified	Auto Single, Dual, Dual Presentation Only, Triple Presentation Only, Triple, Quadruple
Self-View	Unspecified	On, Off
Self-View Position	Unspecified	Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left Lower Right
Wallpaper	Unspecified	None, Custom, Growing, Summer Sky, Waves, Blue

Menu	Section	Options
Duration	CamCtrlPip CallSetup	1–60
Mode	CamCtrlPip CallSetup	On, Off
HDMI1–4 RGB Quantization Range	Input	Auto, Full, Limited
DVI 3, 5	Input	RGB Quantization Range, Type (Auto Detect, Digital, Analog RGB, Analog YPbPr)
Source 1–5	Input	Connector, Name, Presentation Selection, Quality, Type, Visibility, Camera ID, Mode, Optimal Definition Profile, Threshold 60 fps
Disable Disconnected Local Outputs	Layout	On, Off
Local Layout Family	Layout	Auto, Full Screen, Equal, Presentation Small Speaker, Presentation Large Speaker, Prominent, Overlay, Single
Presentation Default View	Layout	Default, Minimized, Maximized
Remote Layout Family	Layout	Auto, Full Screen, Equal, Presentation Small Speaker, Presentation Large Speaker, Prominent, Overlay, Single
Scale to Frame	Layout	Manual, Maintain Aspect Ratio, Stretch to Fit
Scale to Frame Threshold	Layout	0–100
Scaling	Layout	On, Off
Auto Select Presentation Source	OSD	On, Off
Call Settings Selection	OSD	On, Off
Encryption Indicator	OSD	Auto, Always On, Always Off
Language Selection	OSD	On, Off
Login Required	OSD	On, Off
Menu Startup Mode	OSD	Home, Closed
Missed Calls Notification	OSD	On, Off
Mode	OSD	On, Off
My Contacts Expanded	OSD	On, Off

Menu	Section	Options
Output	OSD	Auto, 1-4
Today's Bookings	OSD	On, Off
Virtual Keyboard	OSD	User Selectable, Always On
Wallpaper Selection	OSD	On, Off
Input Method Cyrillic	OSD	On, Off
Input Language	OSD	Latin, Cyrillic
Composite 5	Output	Monitor Role, Over-Scan Level, Resolution, Location Horizontal Offset, Location Vertical Offset
DVI 2 and 4	Output	Monitor Role, Over-Scan Level, Resolution, RGB Quantization Range, Location Horizontal Offset, Location Vertical Offset
HDMI 1 and 3	Output	CEC Mode, Monitor Role, Over-Scan Level, Resolution, Location Horizontal Offset, Location Vertical Offset
Active Speaker Default Value Position	PIP	Current, Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left Lower Right
Presentation Default Value Position	PIP	Current, Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left Lower Right
Full Screen Mode	Self-View Default	Current, Off, On
Mode	Self-View Default	Current, Off, On
On Monitor Role	Self-View Default	First, Second, Current, Third, Fourth
PIP Position	Self-View Default	Current, Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left, Lower Right

Validating Network Settings

Network settings are a critical part of configuring any device. "If you can't ping it, you can't ring it" is the coined phrase that best describes the necessity of configuring these network settings appropriately. Some qualifying questions that must be answered before configuring the network settings on a TC software-based endpoint are, "What speed and duplex should be used, and should these settings be discovered automatically or statically assigned?" "How will VLAN discovery be used, if it is used at all?" "Will DHCP be used or static IP addressing?"

The question pertaining to speed and duplex will be addressed first. The speed options available on TC software-based endpoints are 10 Mbps, 100 Mbps, and 1000 Mbps (or 1 Gbps). Duplex has to do with how nodes send and receive packets across a network, and the options are half duplex and full duplex. Both offer two-way communication, but half duplex only allows for communication to occur one direction at a time. Walkie-Talkies are perfect examples of half-duplex communication. What happens if both parties using a Walkie-Talkie try pressing the Talk button at the same time? Neither party will be able to hear what the other party is saying. Full duplex allows for a node to send and receive packets at the same time. In IP communications, only full duplex should be used. Using half duplex in IP communications will double the amount of bandwidth required because extra ports will need to be opened for two-way communication. Duplex is configured and displayed with the speed on TC software-based endpoints. The options available are Auto, 10half, 10full, 100half, 100full, and 1000full. Auto is the default setting and will use whatever speed the router specifies should be used. It is recommended by Cisco that Auto should be used. However, it is always good to verify what rate is actually negotiated. If speed and duplex are configured as Auto, but the status shows half duplex, the setting will need to be changed on both the endpoint and the router to full duplex. If this setting is only changed on one device and not the other, you could experience something called duplex mismatch. Telltale signs that duplex mismatch is occurring include registrations dropping, calls not connecting, or calls dropping in the middle of the call.

Another potentially problematic component pertaining to network settings is VLAN usage. Endpoints in a Cisco Unified CM environment need to use tagged auxiliary voice VLAN. However, when TC software-based endpoints register with the VCS, the untagged data VLAN is used. Even when the untagged data VLAN is used, Cisco Discovery Protocol (CDP) will still discover TC software-based endpoints connected to a switch. However, this does not mean that the endpoint will automatically search for the voice VLAN. The VLAN mode on the endpoint must be set to either Auto or Manual. Auto will allow the endpoint to discover VLAN information using CDP. Manual required an administrator to manually set the tagged auxiliary voice VLAN numeric value. The VLAN mode is automatically changed to auto when the provisioning mode is changed to CUCM. (Review the previous section on registering TC software-based endpoint to the Cisco Unified CM for instructions on how to change the provisioning mode.)

IP addressing information is required when any device wants to communicate across a network. The required components needed are an IP address, default gateway, and the subnet mask. Other optional network addressing information that could be used are DNS addresses and, if Option 150 is used, TFTP server addresses. IP addressing information can be delivered over DHCP, or they can be statically assigned. TC software-based endpoints will use DHCP by default. If an administrator wants to use static IP addressing, these settings can be changed. It is not recommended to change these settings from the web interface because once one component is changed, you may lose connectivity to the endpoint. The best option is to use the CLI with a serial connection or use the remote control. The commands that enable you to configure static network settings with the CLI are as follows:

```
xConfiguration Network 1 IPv4 SubnetMask: 255.255.255.0
xConfiguration Network 1 IPv4 Gateway: "xxx.xxx.xxx.xxx
xConfiguration Network 1 IPv4 Address: xxx.xxx.xxx.xxx
xConfiguration Network 1 IPv4 Assignment: Static
```

To configure IP settings on a TC software-based endpoint using the remote control, navigate to **Home > Settings > Administrator Settings > Advanced Configuration > Network 1 > IPv4**. Click the following menu options to change the settings: **Assignment**, **Address**, **Gateway**, and **SubnetMask**. Figure 10-12 shows how to access these menus using the remote control.

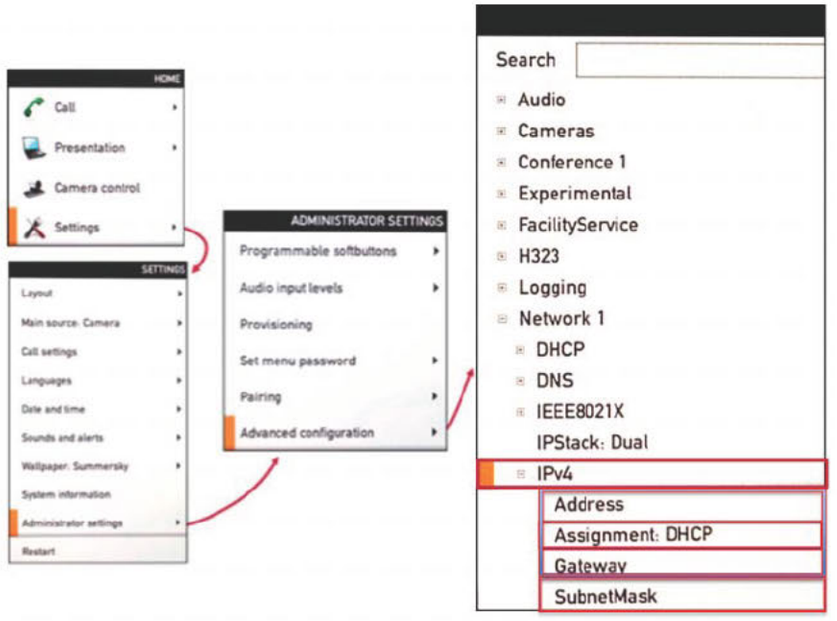


Figure 10-12 *Configuring Static IP Settings with the Remote Control on TC Software-Based Endpoints*

Subscribing to Corporate Directories or Phonebooks

Key Topic

Once all network settings have been configured, audio and video settings have been calibrated, and the endpoints have been registered, calls can now be made. Users can place calls by manually dialing the destination alias or by looking up entries from a directory or phonebook. There are four types of phonebook options on TC software-based endpoints. Users on the TC endpoint define local phonebooks. Aliases from previous calls can be saved into the local phonebook, or manual entries can be created. Endpoints registered to the Cisco Unified CM can receive directory entries from the Cisco Unified CM in an enterprise phonebook. Endpoints registered to the Cisco VCS can receive either corporate phonebooks or global phonebooks from TMS.

If a TC software-based endpoint is registered to the Cisco Unified CM, phonebook settings are automatically configured on the TC endpoint. To verify these settings from the web interface, navigate to **Configuration > System Configuration > Phonebook Server**. The type should automatically be set to CUCM, and the URL should be configured as http://ServerIPAddress:8443/cucm-uds/users. Users can now access directory entries using the remote control (Intelligent Proximity or Touch controller) by selecting the **Home** button and then scrolling to Call and selecting **Phonebook**.

Global phonebooks (also referred to as downloaded phonebooks) and corporate phonebooks (also referred to as centralized phonebooks) are received from TMS in different manners from each other and can only be used in a VCS call control environment. The big difference between these two types of phone books is that global phonebooks are downloaded to the endpoint, whereas corporate phonebooks are centrally located on TMS. Endpoints must be configured to subscribe to TMS before corporate phonebook entries are published to the endpoint. The advantage of global phonebooks is that if the endpoint loses connectivity to TMS, the endpoint still keeps the global phonebook entries. A disadvantage of global phonebooks is the capacity limitations of TC software-based endpoints. Another disadvantage of global phonebooks is directory entries are only as current as the last time the phonebooks were pushed to the endpoint. An advantage of a corporate phonebook is that entries are always current. Also, there is no limit to the number of entries a phonebook can contain because corporate phonebooks reside on TMS at all times. The disadvantage of corporate phonebooks is that if the endpoint loses connectivity to TMS, corporate phonebooks cannot be accessed. Both global and corporate phonebooks can be used on TC software-based endpoints at the same time, so there is no reason an administrator should have to choose which phonebook to use.

No settings need to be configured on a TC software-based endpoint to receive global phonebooks. However, these endpoints do need to be configured with corporate phonebooks so that the endpoint knows where to subscribe to for phonebook entries. To configure corporate phonebook settings from the web interface of TC software-based endpoints, navigate to **Configuration > System Configuration > Phonebook Server**. The type should be set to TMS, and the URL should be configured as http://TMSServerIPAddress/tms/external/phonebook/phonebookservice.asmx. Users can now access corporate phonebook entries using the remote control (Intelligent Proximity or Touch Controller) by selecting the green **Call** button. When users begin typing an alias (or participant name), entries will automatically populate based on the characters dialed. The arrow keys can be used to make a selection from the list.

Cisco TC Software-Based Endpoint Call Scenarios

Users and administrators can call on TC software-based endpoints using the remote control, web interface, CLI Touch controller, or Intelligent Proximity. If the remote control of a Touch controller is used, pressing the green **Call** button will bring up calling options. When placing calls through the web interface, users need to navigate to the Call Control menu. Under the Contacts box, aliases can be entered in the Search or Dial field. Additional options include selecting entries from the Favorites, Directory or Resents categories. When an alias is dialed in the Search or Dial field, a callout window will appear to the right. Within that callout will be a green Call button and a Show Call Settings menu option. Selecting the **Show Call Settings** menu option offers additional Call Rate and Protocol options. Call rate is the bandwidth speed the call will request to use, and protocol options include Auto, H.323, and SIP. If the CLI is used to place calls, the command to use is **xCommand Dial Number:** <*alias*>.

Though placing calls is a fairly intuitive task, several configurable options are available on TC software-based endpoints that relate to calls. Such options include Auto Answer,

Content Sharing, Media encryption, Near/Far End Camera Control, and other call settings. Most of these settings can be configured from the web interface by navigating to **Configuration > System Configuration > Conference**.

Key Topic

The first setting you will find under this menu is the Encryption Mode. These settings can be configured as On, Off, or Best Effort. Best Effort is the default setting, and with this setting configured the endpoint will always try to encrypt the call. If the far-end endpoint does not support the same encryption, or if it has encryption turned off, the call will still connect as an unencrypted call. The On setting requires encryption to be used at all times or else calls will not set up. The Off setting requires encryption to never be used; otherwise, calls will not set up. H.323 uses AES 128-bit encryption on TC software-based endpoints. SIP uses Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) for signaling and media encryption.

Key Topic

Auto Answer is the next menu section available. Options under Auto Answer include Delay, Mode, and Mute. Delay sets a time duration for how long the phone will ring before the call is answered automatically. The default for this setting is 0, it can be set up to 50, and the measurement is in seconds. Mode is how auto answer is enabled. It can be configured as on or off, and the default is off. The Mute option enables users to have the microphone muted automatically when auto answer connects the call. This is a good option to use in collaboration meeting rooms where participants may still be settling in the room while calls are being connected. It can be configured as on or off. Using auto answer could create a potential security threat for eavesdropping. This setting should be used only in certain environments and with caution.

Key Topic

Skipping down a few sections, the Far End Camera Control (FECC) options are available. The two options here are Mode and Signal Capacity, and both can be configured as on or off. On is the default configuration. FECC allows for endpoints you are connected to in a call to pan, tilt, and zoom your camera. Sometime participants do not use the self-view feature on endpoints and are unaware of how they are framed in a camera. Enabling the FECC feature on endpoints allows the participants viewing the far end to adjust the camera as they need to.

Presentation is the next section available. The options under Presentation are OnPlacedOnHold and Relay Quality. OnPlacedOnHold determines whether content being shared will continue after a call is placed on hold. The options for this setting are No Action and Stop. Relay Quality can be configured as Sharpness or Motion. If the content being shared is still image, like a PowerPoint presentation or a Word document, Sharpness should be used so that the quality of the image is the greater priority. If the content being shared involves moving images, like a commercial clip or YouTube video, Motion should be used because the frame will change at a higher rate.

Other call settings can be configured under the Conference menu like the Default Call Protocol and Rate, Do Not Disturb Mode, Video Bandwidth Mode, and many more. All of these calibration settings allow users and administrators to define parameters unique to their environment resulting in the best possible user experience.

Cisco TC Software-Based Endpoint User Accounts

By now, you should understand how to interface with, register, calibrate, and call using TC software-based endpoints. This topic shifts now to what user accounts are available on these endpoints and how TC endpoints can be secured.

Key Topic

It is best to understand what user accounts are available on TC software-based endpoints as they come from the factory. If you have an endpoint that has already been configured, you can perform a factory reset of the endpoint. Unlike Cisco Telepresence Systems (CTS), a factory reset on TC endpoints will not change the firmware load that is on the endpoint. For example, if you bought a C90 when the current software image was running TC4.0, and you upgraded that endpoint to Version of TC7.2, and then performed a factory reset on that endpoint, you will still run the current version of TC7.2. A factory reset on TC software-based endpoints only wipes out the configuration settings. A factory reset can be performed using the Touch control pad, web interface, or the CLI. Using the web interface to perform a factory reset requires an administrator to navigate to **Maintenance > System Recovery**. Click the **Factory Reset** tab, and then click the **Perform Factor Reset** button. A pop-up window will appear asking, "Are you sure you want to perform a factory reset?" Click the red **Yes button**. The endpoint will wipe all the configuration settings and initiate a reboot. Once rebooted, the endpoint will contain only the default settings as it came from the factory. Be aware that the default network settings are configured to use DHCP. If you operate in a static IP environment, the IP address information configured on the endpoint will be lost.

Key Topic

The default user account that exists on a TC software-based endpoint is a full administrator access account. The username is admin, and the password is blank. This account can be secured, and additional user accounts can be created on the endpoint. The role options for additional user accounts are Admin, Audit, and User. Admin gives users full administrator privileges. Audit only give users access to log-related information. User allows users to place calls and change limited settings like wallpaper, ring tone, self-view, and layouts. TC software-endpoints can be secured with a password using the web interface or the CLI. Using the web interface, click the admin name in the top-right corner of the screen, and click the **Change Password** drop-down menu that appears. The page that comes up will display a configuration box for the Current Password, New Password, and Repeat New Password. After filling out the fields, click the **Change Password** button, and the password is changed. To change passwords from the CLI, use the command **xCommand SystemUnit AdminPassword Set Password:** <*password*>.

Key Topic

Changing the password will help prohibit unauthorized personnel from accessing TC software-based endpoints. However, a user can still access administration menus from the remote control, or a hacker could still perform a packet trace and view user login credentials over HTTP and Telnet connections (because they are sent in clear-text format). A PIN can be created that restricts access to administration menus using the remote control. This can be configured using the remote control, web interface, or CLI. To configure these settings using the remote control, navigate to **Home > Settings > Administrator Settings > Set Menu Password**. Enter a numeric PIN and click **Save**. This PIN only restricts access

to the Administrator Settings menus. To create a PIN using the web interface, navigate to **Configuration > User Administration**. Click in the admin account that already exists and scroll to the bottom of the page. Enter the PIN you are creating in the PIN and Repeat PIN fields, and click the **Change PIN** button. To change or set a pin using the CLI, enter the command **xCommand SystemUnit MenuPassword Set Password:** <*password*>.

Key Topic

Secure Shell (SSH) can be turned on and Telnet turned off for added security. In addition, HTTP can be turned off while HTTPS is left on. The easiest way to perform these tasks is to use the web interface and navigate to **Configuration > System Configuration > Network Services**. All the previously mentioned settings are listed under Network Services. For an added layer of security, there is a setting on TC software-based endpoints called Strong Security Mode. This feature was instituted to adhere to policies implemented by the U.S. Department of Defense Joint Interoperability Test Command (JITC) regulations. Enabling strong security mode will require passwords meet certain criteria of length and character usage. They will be required to change every 60 days, accounts can be locked if more that three failed attempts are made to log in, and some features are lost when in use. Also, if the admin account is locked, or the password forgotten, there is no recovery process for that password or the unit. Only an RMA (Return Merchandise Authorization) can be issued to correct the situation. Best practice suggests not using strong security mode unless you have to. Should you want to access this setting, from the web interface navigate to **Configuration > Security** and click the **Strong Security Mode** tab.

Summary

The Cisco TelePresence TC software-based endpoint solution is a user-friendly endpoint solution for businesses and has a diverse selection of product to choose from. These products are feature rich, supporting both H.323 and SIP communication protocols. TC endpoints allow users and administrators to interface with them through multiple applications, including the OSD using the remote control, the Cisco Touch 10 or Touch 8 control pads, the web interface, the CLI, and Intelligent Proximity for Content Sharing. TC software-based endpoints can register with either the Cisco Unified CM using SIP, or they can register with the Cisco VCS using SIP/H.323. Administrators have many options to calibrate TC software-based endpoints to a production environment. Some of those options include audio and video settings, integrating phonebooks, and adjusting network settings. Additional settings can be calibrated for different call scenarios like auto-answer settings, how content is shared, FECC, encryption settings, and many other call-related settings. Finally, creating passwords, leveraging SSH and HTTPS, and enabling the strong security mode can enhance security for TC software-based endpoints.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 10-4 lists a reference of these key topics and the page numbers on which each is found.

Table 10-4 Key Topics for Chapter 10

Key Topic Element	Description	Page Number
Figure 10-1	SIP registration process	221
Figure 10-2	H.323 registration process	223
Figure 10-3	SIP call flow using Early Offer	223
Paragraph	5 ways to interact with TC software-based endpoints	225
Paragraph	How to configure Intelligent Proximity on TC software-based endpoints	230
Paragraph	How to register TC software-based endpoints to the Cisco Unified CM	231
Table 10-2	Audio collaboration options	235
Table 10-3	Video collaboration options	237
Paragraph	Phonebook options on TC software-based endpoints	241
Paragraph	Encryption options on TC software-based endpoints	243
Paragraph	Auto-answer options on TC software-based endpoints	243
Paragraph	Far-end camera control options on TC software-based endpoints	243
Paragraph	How to perform a factory reset on TC software-based endpoints	244
Paragraph	Admin account on TC software-based endpoints and how to secure it with a password	244
Paragraph	How to secure a TC software-based endpoint using a PIN	244
Paragraph	How to secure a TC software-based endpoint using HTTPS and SSH	245

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

SIP, SIP server, SIP proxy, SIP registrar, H.323, H.323 gatekeeper, interworking gateway, FQDN, DN, CAC, SDP, RAS, GRQ/GCF, RRQ/RCF/RRJ, ARQ/ACF/ARJ, H.225, Q.931, H.245, OSD, PIP

This chapter covers the following topics:

- **NAT and Firewall-Traversal Overview:** This section provides an overview NAT and firewall issues, and how these issues have been addressed in a collaboration environment.
- **Solution Overview and Components:** This section examines the Cisco firewall-traversal solutions available on the market today.
- **Mobile and Remote Access:** This section examines how the Cisco collaboration edge solution addresses mobile and remote-access issues for businesses.
- **Jabber Guest:** This section explains how the Jabber Guest solution works and what components are needed to use Jabber Guest.
- **Configuring Call Mobility:** This section provides an overview of the two call mobility options in a Cisco infrastructure environment that allow other users to contact your devices with a single-number-reach solution.

CHAPTER 11

Cisco Legacy Edge Architecture

When networking was first introduced, many companies were formed establishing different types of networks, each using a different language to communicate. Therefore, organizations were established to standardize how devices communicate between each other. Once businesses could communicate together, security had to be introduced to protect these businesses from cyber-attacks. This raised several more communication issues that took many years to resolve. Cisco has an iron-clad solution that allows business to communicate with one another, and with customers, in a secure environment.

This chapter discusses Network Address Translation (NAT) and firewall issues that companies encounter within a collaboration solution. An overview of Cisco solutions that address these issues will help you understand the foundational components needed in a Cisco firewall-traversal solution. This solution enables remote and telecommuters to establish mobile and remote access to infrastructure within an organization. You will also learn how business-to-consumer communication can be established using the Cisco Jabber Guest solution. All of these components can be interlaced together with an explanation on how different call mobility solutions function, and how they can be configured to establish a single-number-reach for users with multiple modes of communication.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 11-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 11-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
NAT and Firewall-Traversal Overview	1–5
Solution Overview and Components	6–7
Mobile and Remote Access	8–9
Jabber Guest	None
Configuring Call Mobility	10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What type of address is 192.168.192.168?

   a. Class B public IP address
   b. Class B private IP address
   c. Class C public IP address
   d. Class C private IP address

2. An SX20 sitting on the public Internet, configured to use H.323 in direct mode, tries to call another SX20 sitting in a private network, also configured to use H.323 in direct mode. What is the expected outcome?

   a. The destination endpoint will never ring.
   b. The destination endpoint will ring, but the call will drop immediately after the call is answered.
   c. The destination endpoint will ring, and call setup will occur, but the media will be one-way, resulting in the call dropping eventually.
   d. The destination endpoint will ring, call setup will occur, and the media will flow bidirectionally between the two endpoints without issue.

3. Which of the following statements is true about NAT traversal?

   a. STUN is hardware intensive because all call media must go through this server.
   b. TURN is hardware intensive because all call media must go through this server.
   c. ICE is hardware intensive because all call media must go through this server.
   d. ICANN is hardware intensive because all call media must go through this server.

4. What organization created and is responsible for the administration of the Interactive Connectivity Establishment protocol?

   a. ITU
   b. ISO
   c. IEEE
   d. IETF

5. What UDP ports need to be opened on a firewall if H.460.18 is used for firewall traversal?

   a. No ports need to be opened. They will be opened dynamically.
   b. 5060 and 5061.

c. 2776 and 2777.

d. 50000 to 52400.

6. What are the total number of ports that need to be opened when Cisco Assent is used for firewall traversal?

a. 1

b. 2

c. 3

d. 4

7. What products are used in the Cisco collaboration edge solution for firewall traversal?

a. VCS Control and VCS Expressway

b. Expressway Core and Expressway Edge

c. Cisco Unified CM and VCS Expressway

d. Cisco Unified CM and Expressway Edge

8. What is the Cisco Unified Mobility and remote-access solution?

a. Allows Cisco collaboration endpoints outside the enterprise network to register internally to the Cisco Unified CM

b. Allows for the integration of mobile phones with the Cisco Unified CM

c. Allows administrators to configure and change settings on the Cisco Unified CM from remote locations

d. Allows Cisco collaboration endpoints outside the enterprise network to register to an edge call control server

9. Which of the following is a critical component to the Cisco Unified Mobility and remote-access solution?

a. A DMZ is required for the solution to work.

b. A TURN server is required for the solution to work.

c. A certificate server is required for the solution to work.

d. Nothing special is needed for the solution to work.

10. Which call mobility option requires an alias to be configured that is not assigned to an endpoint already?

a. FindMe

b. Cisco Unified Mobility

c. Single number reach

d. One button to push

Foundation Topics

NAT and Firewall-Traversal Overview

The Institute of Electrical and Electronic Engineers (IEEE) first introduced communicating using packet-switched technology in 1974. Several Internet Protocol versions were experimented with (IPv1–3) until the predominant protocol was established circa 1981, called IPv4. At the time, engineers could not imagine the four billion addresses made available with IPv4 would ever run out. Initially, anyone could purchase IP addresses in pools, and they would own them for life. Telco companies and universities were some of the main consumers of these IP addresses. As the number of devices that require an IP address greatly increased, and the World Wide Web began to expand, it was realized that the number of people and devices requiring an IP address would soon eclipse the finite number of IPv4 addresses available. One solution to this problem was the introduction of IPv6, which contains 340 undecillion addresses. Some say you could assign an IPv6 address to every grain of sand on earth and still not run out of addresses. However, IPv6 introduces other issues, like how do you migrate hundreds of millions of devices over to an IPv6 network that are already established under IPv4. Another resolution that came about around the same time as IPv6 was Network Address Translation (NAT).

The Internet Engineering Task Force (IETF) came up with RFC 2663 outlining the basic use of NAT. For NAT to work IP addresses first had to be divided into two pools; Public and Private IP addresses. Internet Cooperation for Assigned Names and Numbers (ICANN) was created in 1998 to assume responsibility for managing IP addresses and domains. Private IP addresses are designated in the following categories, which anyone can use and are not routable across the public Internet. The ranges for private IP addresses are as follows:

- Class A addresses 10.0.0.0 – 10.255.255.255 (16,777,216 available addresses)
- Class B addresses 172.16.0.0 – 172.31.255.255 (1,048,576 available addresses)
- Class C addresses 192.168.0.0 – 192.168.255.255 (65,536 available addresses)

Public IP addresses are routable across the public Internet and can be leased from an Internet service provider. Today there are different versions of NAT and Port Address Translation (PAT) that should be used based on the equipment within a network. However, the basis of how NAT works is that a private IP address is masqueraded with a public IP address when a device needs to route across the public Internet. Your router will mark the packets going out with a virtual port number to enable rerouting return traffic that comes back from the desired destination. For example, if a computer assigned to a private IP address of 10.10.1.14 tries to navigate to Cisco.com, the router will masquerade that private IP address with its assigned public IP address of 209.165.201.1:12345. When Cisco returns communication to the computer, return traffic will go to the public facing port of the router, but the port indicates to the router where to send the return traffic based on a table the router keeps. The router will then change the destination address from 209.165.201.1:12345 to the private IP address of the endpoint, 10.10.1.14, and route the packets from Cisco to the computer that initiated the communication. This type of communication is known as TCP (Transmission Control Protocol). TCP is a two-way communication, meaning that when

packets are sent out, TCP requires a return communication. If a return communication is not received in a set amount of time, the packets are re-sent.

NAT becomes an issue with collaboration devices for two reasons:

- NAT does not allow communication to be initiated from outside the private network because the virtual ports can change with each new transmission that is created. So if two video endpoints behind different NATs want to communicate, one will never be able to discover the other. For example, if a device were to try to route to the private IP address of another endpoint, the transmission would fail at the source router because private IP addresses are not publicly routable. Alternatively, if the source device were to try to route to the public IP address of the far end router, once the packets arrived, the far end router would not know which device to route the packets to.
- The second issue that comes with NAT has to do with UDP (User Datagram Protocol) transmissions. Whereas TCP communications require a response, UDP communications are unidirectional. Once video calls are set up using TCP, the audio and video packets are sent using UDP. Therefore, the one-way transmission has no way of knowing whether the endpoint residing behind the NAT server received the audio or video packets.

The IETF, who came up with the Session Initiation Protocol (SIP) communications protocol and NAT, also came up with the first solution that allowed communications between private LAN/WANs through a NAT server. That protocol is known as Session Traversal Utilities for NAT (STUN). After creating the RFC for STUN, The IETF came up with two other RFC protocols known as Traversals Using Relays around NAT (TURN) and Interactive Connectivity Establishment (ICE). Figure 11-1 illustrates how STUN can be used for NAT traversal.

As illustrated in the scenario in Figure 11-1, the endpoint sends a STUN request through the default gateway to the STUN server located on the public network. The STUN server is listening on port 5060. The gateway forwards the request to STUN server and changes port 5060 to another port number. The STUN server records the address and port and sends a response back to the endpoint. This IP and port are now assigned to the requesting endpoint. When the endpoint establishes a session (for example, a SIP-based Voice over IP [VoIP] or video call with an external entity), it can notify the external entity to sends responses back on the public IP address and port assigned by the STUN server. Now the UDP connection can successfully be established between two endpoints without NAT issues hindering the connection.

Although STUN is a great solution, it does not work properly with networks using Symmetric NAT. Symmetric NAT creates a new address and port mapping each time an internal host tries to connect to an external host. To resolve Symmetric NAT issues, the IETF came us with another protocol called TURN.

TURN performs much like STUN; however, it uses a relay that STUN does not possess, allowing for server-reflexive addresses and SNATs (Symmetric NATs) alike. Because the TURN server is used as a relay, more bandwidth is required, and all media must go through the TURN server. Figure 11-2 illustrates how a TURN server can be used within a network.

Key Topic

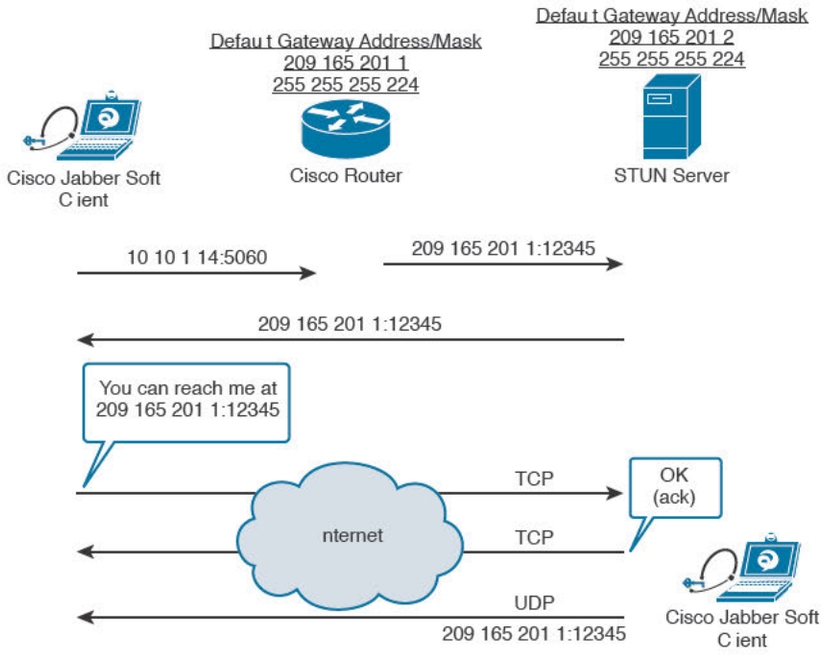


Figure 11-1 *NAT Traversal Using STUN*

Key Topic

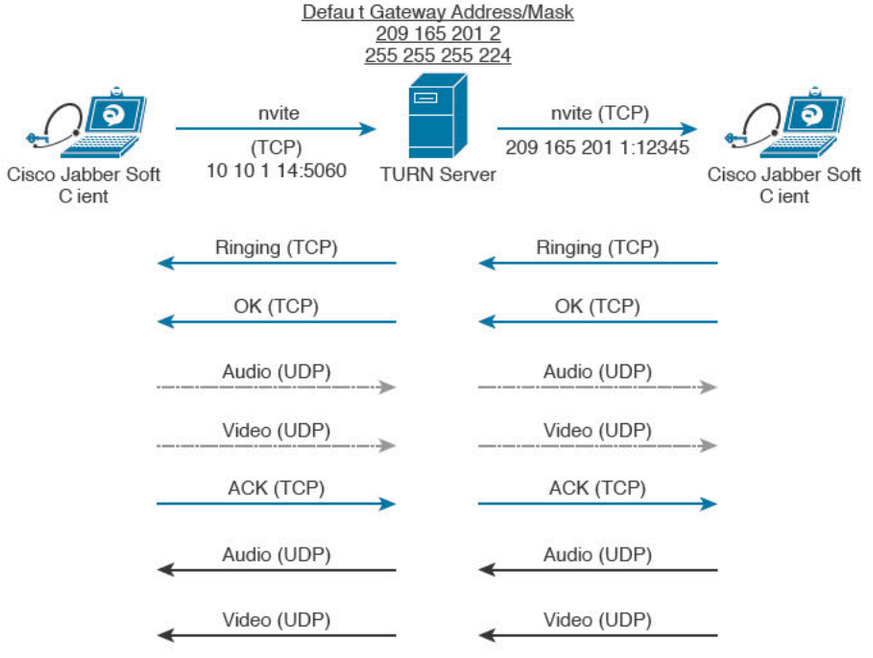


Figure 11-2 *NAT Traversal Using TURN*

This creates issues when two devices are trying to communicate that are within the same network but behind different NATs. For this type of scenario, STUN is a more appropriate choice. Also, because TURN is more hardware sensitive, it is a better solution for larger corporations, but STUN is better suited for smaller companies and home users. Other variables make choosing between them difficult, as well, so the IETF came out with a third option for NAT traversal called ICE.

ICE is the culmination of both STUN and TURN. Based on the type of communication being used and the type of NAT that exists, an ICE server chooses the appropriate traversal solution to use. When communication is trying to be established between two peers, ICE collects all IP information it can and then in turn attempts to established communication with each protocol, based on how the server has been configured. Typically, ICE attempts STUN first, then TURN if communication is not established. Figure 11-3 illustrates how ICE can be used within a network to choose whether STUN or TURN is leveraged.

Key Topic

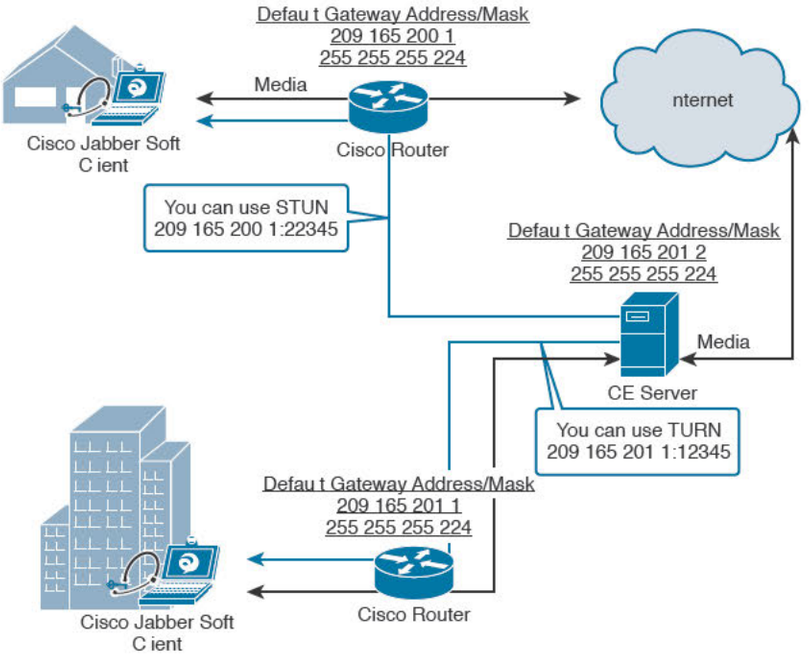


Figure 11-3 *NAT Traversal Using ICE*

Although the IETF helped overcome a great issue with NAT, there are still some limiting factors to the STUN, TURN, and ICE solutions. First, these protocols can be used only in SIP environments. H.323 is not supported with any of them. Also, STUN, TURN, and ICE are only NAT-traversal resolutions and cannot perform firewall traversal. Tunnels must be created through firewalls for any of these protocols to be used.

A firewall is a hardware or software network device that controls what traffic can enter and exit a network. Using firewalls helps protect devices, like computers, from cyber-attacks, which are growing more prevalent every day. The issue with firewalls is similar to that of

NAT. As long as a TCP communication is initiated from behind the firewall to a device outside the firewall, a communication session can be established. However, once that session changes to send and receive UDP packets, inbound media will be blocked. Therefore, two-way communication through a firewall is not possible without some sort of firewall-traversal solution.

TANDBERG had been a leader in video telepresence for many years prior to the Cisco merger. They climbed this ladder to success much the same way as Cisco, by acquiring key companies that possessed the technology they needed for the time. In 2004, TANDBERG acquired a company called Ridgeway Systems and Software, a UK-based software company specializing in firewall and NAT traversal.

The way Assent works requires two components: a traversal server and a traversal client. The traversal server resides outside the firewall (or in a demilitarized zone [DMZ]). The traversal client resides inside the firewall and initiates communication with the traversal server. Ports do need to be opened on the firewall, but they cannot be used unless a communication is initiated from inside the firewall. This is where the magic happens. The traversal client sends a keepalive message to the traversal server, essentially asking, "Do you have any calls for me?" Should someone initiate a call from outside the firewall through the traversal server, that server can respond to the keepalive message sent from the traversal client. As far as the firewall is concerned, the communication initiated from inside the firewall with the keepalive message. Now the ports allocated can be used once the call setup has completed. Even better, though, are the ports needed for media using Assent. Only two ports are required to be opened on the firewall, because Assent will multiplex the media so that all Real-time Transport Protocol (RTP) traffic uses one port, and all RTP Control Protocol (RTCP) traffic uses a second port. In addition to the firewall-traversal capabilities of Assent, NAT traversal is built in to the protocol as well.

Assent is such a powerful tool, that the ITU used it as the basis to develop three H.323 traversal standards known asH.460.17, H.460.18, and H.460.19. By the summer of 2005, the standards were completed and in full use. H.460.17 performs firewall traversal by carrying the media over TCP ports instead of UDP. H.460.18 works just like Assent, except it required ports 50000 to 52400 to be opened on the firewall. In conjunction with H.460.18, H.460.19 multiplexes the media ports so only two ports need to be opened for RTP and RTCP media streams. In this, H.460.18 and H.460.19 accomplish together what Assent is capable of independently. Table 11-2 identifies the ports needed for Assent as compared to H.460.18/.19.

Key Topic

Table 11-2 Assent and H.460.18/.19 Ports Needed

Protocol	Assent	H.460.18 and H.460.19
RAS (UDP port)	1719	1719
Q.931 (TCP port)	2776	1720
H.245 (TCP port)		2777
RTP (UDP port)	2776	2776
RTCP (UDP port)	2777	2777

Cisco NAT and Firewall-Traversal Solution Components

Two Cisco firewall and NAT-traversal solutions are available on the market today. One is based on a Cisco Video Communication Server (VCS)-centric call control platform. The other is based on the Cisco Unified Communications Manager (CM)-centric call control platform. Both solutions can be used together as well, for a complete unified collaboration solution.

Key Topic

The Cisco VCS-centric firewall and NAT-traversal solution comes in two servers. The VCS Control is intended to act as the main internal call control server and acts as the traversal client. Its counterpart, the VCS Expressway, sits outside the firewall, ideally in a DMZ, but retains the same functionality as the VCS Control. The two servers work together to offer a secure firewall and NAT-traversal solution for both H.323 and SIP protocols.

Key Topic

A Cisco Unified CM-centric environment allows for the registration of unified collaboration endpoints like VoIP UC phones along with video TelePresence endpoints. Two immersive TelePresence endpoints Cisco offers, the TX9000 and the IX5000, can also register to the Cisco Unified CM. The Cisco Unified Border Element (CUBE) can function as a TURN server, and has been available for a long time. It offers a versatile deployment of the Cisco Unified CM, establishing a SIP trunk to a service provider for IP-to-PSTN (public switched telephone network) communications. However, Cisco has struggled to establish a solid firewall-traversal solution. After acquiring TANDBERG, Cisco leveraged the VCS-traversal solution to produce a unique product architecture that allows for firewall traversal in a Cisco Unified CM-centric environment. This solution is known as the collaboration edge architecture, or Expressway series products.

The Cisco Expressway series is available starting with Version x8.1. The VCS and Expressway series are similar because the Expressway series was built off of the same software kernel. As far as call control goes, they both function the same; however, they each offer different features beyond call control. The VCSs support registration from H.323 and SIP endpoints, but Expressway series devices do not. The Expressway series is targeted for environments with the Cisco Unified CM as the center of call control. The VCS-traversal solution can still be used in conjunction with the Cisco Unified CM by building a SIP trunk between the Cisco Unified CM and the VCS Control, but using the Expressway series offers additional features.

The Expressway series offers a secure virtual private network (VPN)-less solution for unified communications, known as Mobile and Remote Access. Like the VCS firewall-traversal solution, the Expressway series solution consists of two devices: the Expressway-C (Core) and Expressway-E (Edge). The Expressway series offers the ability to act not only as a video gateway but also as a collaboration gateway for external communications. It enables mobile and remote access for users outside the firewall, and allows for business-to-business (B2B) or business-to-customer (B2C) communication. It is important to note that the B2B and B2C function required Rich Media Session license, also know as the Traversal Call License. Also, a dedicated Expressway-C and Expressway-E must be used for Jabber Guest, but that topic is discussed later.

Regardless of whether the VCS Control and VCS Expressway are used for firewall traversal, or the Expressway Core and Expressway Edge are used, the process for firewall-traversal calls is the same. Firewall traversal offers secure communications across firewalls as follows:

1. The traversal client initiates an outbound traversal connection through the internal firewall to specific ports on the traversal server with secure login credentials.
2. Once the connection has been established, the traversal client sends keepalive packets periodically to the traversal server to maintain the connections.
3. When the traversal server receives an incoming call request from the outside, it sends the request to the traversal client through the existing traversal connection.
4. The traversal client processes the call, and media streams are set up over the existing traversal connection.

Mobile and Remote Access

Unified Communications Mobile and Remote Access is a core part of the Cisco collaboration edge architecture. It allows endpoints, such as Jabber, to securely register, place calls, send instant messages, and obtain presence information that is provided by Cisco Unified CM while the endpoint is located outside the enterprise network. All this is done without having to provide a VPN connection back to the internal network by using the Cisco Expressway series components.

Unified Communications Mobile and Remote Access offers a consistent experience to clients such as Cisco Jabber and Cisco TelePresence EX, MX, and SX series, regardless of whether they are in the internal network or on an external network. It also offers secure communications to other businesses.

Unified Communications Mobile and Remote Access consist of four main components:

- **Firewall-traversal services:** Unified Communications Mobile and Remote Access supports internal firewalls between Cisco Expressway Core and Cisco Expressway Edge. An external firewall between the Cisco Expressway Edge and the Internet can be traversed using two options Cisco offers. You could simply open ports on the firewall and use TURN for NAT traversal, or you can enable the Dual Network Interface option by ordering a special key. The second option is by far more secure.
- **DNS records:** Internal and external DNS records are essential to enable endpoints to detect whether they should register directly with the Cisco Unified CM or through Unified Communications Mobile and Remote Access.
- **Certificates:** Unified Communications Mobile and Remote Access provides secure communication over Transport Layer Security (TLS). Trust between TLS entities is established based on certificates. Implementing the necessary certificates for a Private Key Infrastructure (PKI) is an important part of Unified Communications Mobile and Remote Access implementation.
- **Reverse HTTPS Proxy:** To support secure data services, such as visual voice mail, contact photo retrieval, Cisco Jabber custom tabs, and so on, a reverse HTTPS proxy runs on the Cisco Expressway Edge server.

Unified Communications Mobile and Remote Access uses the same firewall-traversal mechanism as the VCS Control and Expressway to allow inbound- and outbound-initiated packet exchange. Both the VCS Control with the VCS Expressway, and the Expressway Core with the Expressway Edge, leverage this firewall traversal for external calling. However, Unified

Communications Mobile and Remote Access also allows the traversal communication to be leveraged for endpoint registration. Unified Communications Mobile and Remote Access uses the Expressway Edge as the traversal server that is installed on the public network or in a DMZ and Expressway Core as the traversal client that is installed on the internal network. The following connections must be enabled on the firewall:

- **Internal firewall between Cisco Expressway Core and Cisco Expressway Edge**
  - **SIP:** TCP 7001
  - **Traversal Media:** UDP 36000 to 36001
  - **Extensible Messaging and Presence Protocol (XMPP):** TCP 7400
  - **HTTPS (tunneled over Secure Shell (SSH) between Expressway Core and**
  - **Expressway Edge):** TCP 2222
- **External Firewall between the internet and Cisco Expressway Edge**
  - **SIP:** TCP 5061
  - **HTTPS:** TCP 8443
  - **Extensible Messaging and Presence Protocol (XMPP):** TCP 7400
  - **Traversal Using Relay NAT (TURN) server control and media:** UDP 3478 / 6000 to 61799
  - **Media:** UDP 36012 to 59999

The external DNS server must be configured with collab-edge._tls.<domain> service records so that external endpoints can discover that they should use Cisco Expressway Edge for mobile and remote access. Service records for secure SIP are also recommended for deploying secure SIP calls on the Internet. The service records must point to the Cisco Expressway Edge server.

The internal DNS server must be configured with a cisco-uds._tcp.<domain> service record so that internal endpoints can discover that they should use Cisco Unified CM for direct registration. Be sure that the uds service records are not advertised externally; otherwise, issues could result from clients not knowing where to register. When using Cisco Unified CM IM and Presence, a cuplogin._tcp<domain> service record is also required on the internal DNS. You must point all call-processing nodes to a Cisco Unified CM cluster fully qualified domain name (FQDN) when configuring the cisco-uds._tcp.<domain> service record. All Cisco Unified CM IM and Presence server clusters should be configured in the same manner when configuring the cuplogin._tcp.<domain> service record. The internal DNS records must be available to all internal endpoints and to Cisco Expressway Core.

Unified Communications Mobile and Remote Access requires certificates for secure communication between endpoints outside the network and the internal Cisco Unified CM. Cisco has recently issued four new certificates to use in conjunction with the Expressway Edge or the VCS Expressway. Though these new certificates pertain to WebEx integration, Cisco recommends they be used regardless of whether WebEx is being used. These four certificated are not included in Table 11-3, which outlines the different certificate types needed and where they are needed.

Key Topic

Table 11-3 Certificate Types Used in an Expressway Edge Solution

Certificate Type	Core	Edge	Comments
Public or enterprise certificate authority (CA) certificate chain to sign Expressway Core certificate	Y	Y	Required to establish traversal zone connection
Public or enterprise CA certificate chain to sign Expressway Edge certificate	Y	Y	Required to establish traversal zone connection
Cisco Unified CM Tomcat certificates or CA chain	Y	N	Only required when Expressway Core configured to use TLS verify mode on Cisco Unified CM discovery
Cisco Unified CM CallManager certificates or CA chain	Y	N	Only required when Cisco Unified CM is in mixed mode for end-to-end TLS
Cisco Unified CM IM and Presence Tomcat certificates or CA chain	Y	N	Only required when Expressway Core configured to use TLS verify mode on IM and Presence discovery
Cisco Unified CM CAPF certificate or certificated	N	Y	Only required when remote endpoints authenticate with a locally significant certificate (LSC)

The HTTPS Reverse Proxy is a function that is provided by the Cisco Expressway Edge. It is required for certain data applications such as visual voice mail and contact photo retrieval. It provides a mechanism to support visual voice-mail access, contact photo retrieval, and Jabber custom tabs. Reverse Proxy is available on the Cisco Expressway Edge server on TCP port 8443 for HTTPS traffic. Initial mobile and remote access configuration allows inbound authenticated HTTPS requests to the following destinations on the internal network:

- TCP 6970 (TFTP file download) and TCP 8443 (UDS API) to all discovered Cisco Unified CM nodes
- TCP 7400 (XCP router) and TCP 8443 (SOAP API) to all discovered Cisco IM and Presence nodes

The Unified Communications Mobile and Remote Access provides service discovery on the public network. The service discovery occurs as follows:

1. Cisco Jabber sends a DNS SRV record lookup for cisco-uds._tcp.<domain> to a public DNS.
2. The public enterprise DNS that manages <domain> would not have such an SRV record because it is used within internal DNSs, and therefore the lookup fails. Cisco Jabber now sends another DNS SRV record lookup for collab-edge._tls.<domain>. This time the lookup is successful, and the IP address of the Cisco Expressway Edge server is provided to the Cisco Jabber client in the DNS response.
3. Cisco Jabber client starts the mobile and remote-access negotiation with the Cisco Expressway Edge server.

4. If a CA server does not sign the certificate, the Cisco Jabber certificate may need to be manually trusted by the user. A TLS handshake is exchanged to establish a secure connection.
5. When the connection between Cisco Jabber and Cisco Expressway Edge is established, Cisco Jabber tries to register to the services that are enabled on Cisco Expressway Core, which in this case is Cisco Unified CM.
6. The registration request from Cisco Jabber is then sent to Cisco Unified CM by the Cisco Expressway series devices.

Figure 11-4 illustrates the Unified Communications Mobile and Remote Access service discovery.

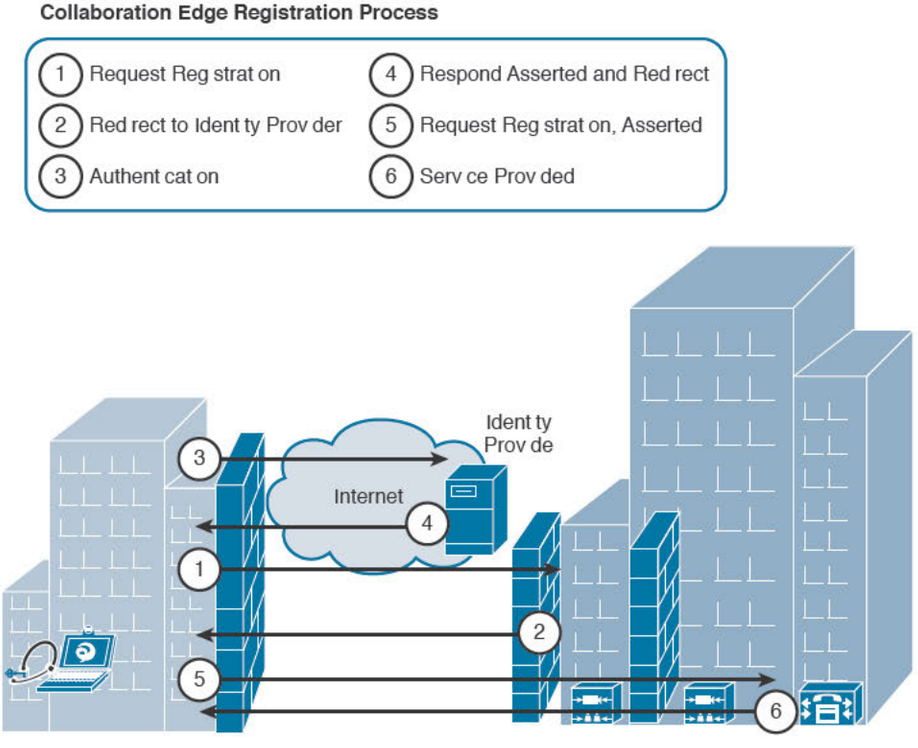


Figure 11-4 *Unified Communications Mobile and Remote Access Service Discovery*

A variety of endpoints are now supported through the Unified Communications Mobile and Remote Access solution. Jabber client has been supported since the products first launched. TC software-based endpoints, like the SX10, SX20, SX80, MX200G2, MX300G2, MX700, and MX800, have also been supported for some time using the Collaboration Edge solution. As of 2015, several new products have been added to the lineup. The 7800 and 8800 VoIP phones can now support a VPN-less connection to the Cisco Unified CM. Also, the DX series endpoints can register through the Expressway Core and Expressway Edge.

Note It is important for users to be aware that by default, when a Jabber IM client is being used, it will try to authenticate with WebEx Connect first, regardless whether the customer is using WebEx Connect. You can call Cisco, or your service provider, and have them disable it.

Jabber Guest

Cisco has a new product available through the collaboration edge solution that helps businesses extend their reach to customers who may not have a video communication solution available. Cisco Jabber Guest helps customers interact with enterprise workers by using real-time communications that are high quality, standards based, and comprehensive. Enterprise workers can send a link to guests, who simply need to click a URL link, website link, or mobile application to start the interaction. This will start a WebRTC type of a session with the employee using a Cisco collaboration endpoint. Build these capabilities in to your website or mobile application with the included software development kits (SDKs), or use the Jabber Guest client experiences. With Cisco Jabber Guest, different user-friendly options still exist, like audio and video communication. Desktop- and content-sharing capabilities are not available currently, but receiving content is coming in a future release. Guest users are not required to enter a username or password because there is no account needed for those users to employ Jabber Guest.

Cisco Jabber Guest allows organizations to leverage an already-existing infrastructure. There is a Jabber Guest server that needs to be deployed before these services are available. Also, the Cisco Jabber Guest solution requires a dedicated Expressway Edge and Expressway Core. Various deployment options exist with this solution, but the simplest way Jabber Guest works is in a Cisco Expressway Edge with single network interface card (NIC) deployment. Within the enterprise network resides the Cisco Unified CM, the Expressway Core, and the Jabber Guest server. Endpoints register to the Cisco Unified CM because the Cisco Unified CM still handles all the call control between these endpoints and the Jabber Guest client. The Expressway Edge server lives outside the internal firewall, possibly in a DMZ. Customers can launch Jabber Guest within their own network using a browser like Firefox or Google Chrome. When the customer launches a Jabber Guest call, the call setup signaling crosses the Internet to the Cisco Expressway Edge server. The Expressway Edge passes the signaling to the Expressway Core, and the Expressway Core first establishes a communication with the Jabber client server to determine how it should route this session. Then the Expressway Core communicates with the Cisco Unified CM. All call admission control settings are applied to this call before the Cisco Unified CM communicates with the collaboration endpoint that a call attempt is being made. Return call setup communication follows the same path in reverse order. Once the call is set up, the media flows from the Jabber Guest client to the collaboration endpoint and back again, through the Expressway Core and Edge. Figure 11-5 illustrates how the Cisco Jabber Guest solution works.

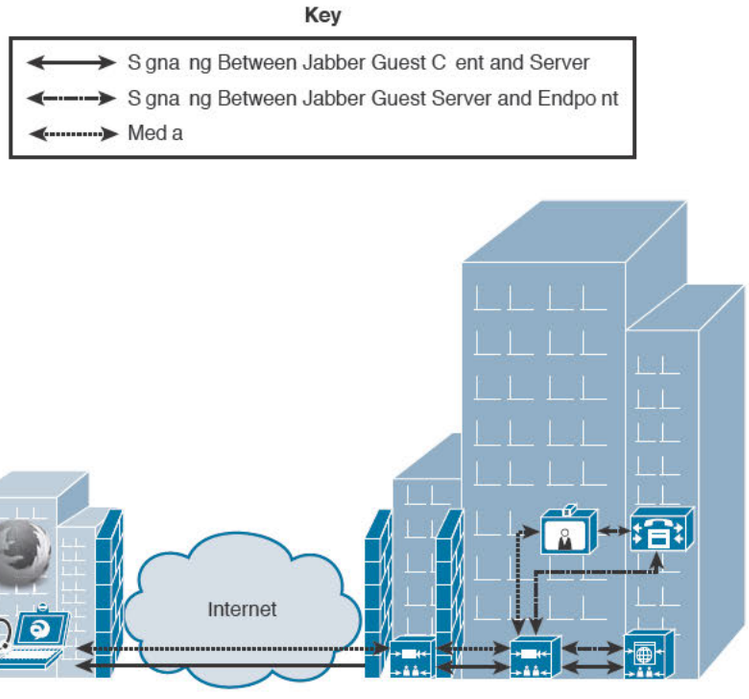


Figure 11-5 *Cisco Jabber Guest Call Setup Process*

Configuring Call Mobility

Key Topic

Call mobility is a service that allows multiple phones to ring at the same time. This feature allows enterprise workers to be contacted by anyone who calls them, regardless of where they are. Two call mobility options available are in a Cisco collaboration solution. Cisco Unified Mobility (formerly known as One Number Reach) is available in a Cisco Unified CM-centric environment. The second call mobility option, FindMe, is available in a Cisco TelePresence VCS-centric environment.

Unified Mobility is a feature included with the Cisco Unified CM. Multiple aliases can be associated with a single endpoint's alias. When that alias is dialed, the call-forwarding intelligence in Cisco Unified CM forwards the call to all the devices associated with the dialed alias. The first endpoint the user answers will connect the call, and all other devices will no longer ring. Different controls can be implemented, such as call-forwarding specifications and ring durations. Integration over the PSTN can be implemented, and the Collaboration Edge solution can play a viable part in the Cisco Unified Mobility service as well.

Each end user can configure Cisco Unified Mobility to his or her own specifications. To log in to the Self Care Portal on the Cisco Unified CM, navigate to https://CUCM name or IPaddress>/ucmuser. Enter the user login credentials when prompted. The Cisco Unified CM system administrator, who also controls what features are available, must set up use of the Self Care Portal before end users can configure their settings. However, once users log in, there are several functions they could potentially perform. End users can modify the mobile number, allowing a cell phone to ring when the primary number is dialed. End users can control the timers, which are used to control the mobility algorithm. Time schedules can be established that determine which devices will ring during different hours and days. For example, Monday through Friday from 9:00 a.m. to 5:00 p.m., a user's mobile phone, DX70 desk phone, and Jabber client will all ring for 30 seconds; then the call will redirect to voice mail. All other hours, the call will go directly to voice mail. Certain callers can also be blocked from calling Unified Mobility devices.

Similar to Unified Mobility, FindMe is a call mobility feature for Cisco VCS-centric environments. Using FindMe requires an option key. The operation of FindMe is very similar to Cisco Unified Mobility. One significant difference between the two call mobility features is the alias used to extend reachability. Cisco Unified Mobility uses the alias of the primary endpoint to initiate the transfer of the call. FindMe requires a FindMe ID to be configured for the FindMe account, which is the dial-able alias to be used. When a user dials the FindMe ID, the VCS initiates a call-processing order. Within the call-processing order, the alias dialed is identified as a FindMe ID, and the call transfer behaviors will be based on the FindMe account with which it is associated. The first behavior the VCS looks for in a FindMe account is what endpoint, or endpoints, the call should be transferred to first. There are two alternate options of transfer based on the behavior of the first call transfer. If the call is busy another endpoint, or endpoints, can be specified for the call to be transferred. Alternatively, if the call rings for a specified duration of time without being answered, another selection of devices can be specified to transfer the call.

Whereas Cisco Unified Mobility has a Self Care Portal for users to configure their Unified Mobility settings, Cisco FindMe has a user portal as well. How this portal is accessed will depend on how the VCS-centric environment is set up. FindMe is a feature of the Cisco VCS. Navigating to the URL or IP address of the Cisco VCS will present two login options: Administrator or User. The User login is how FindMe uses can log in to manage their own FindMe accounts. Cisco TelePresence Management Suite (TMS) can play an active role in how FindMe works. If TMS Provisioning Extension (TMSPE) integration is used, the User login portal through the VCS goes away, and a new User portal is made available through TMS. FindMe accounts are created initially by the VCS administrator, and then configured by users to their desired specifications. Because organization may need to support thousands of FindMe accounts, TMS integration can be used to provision a FindMe template, which can be mass distributed to everyone within an organization. Figure 11-6 illustrates the FindMe user portal on the VCS as it compares to the FindMe user portal on TMS.

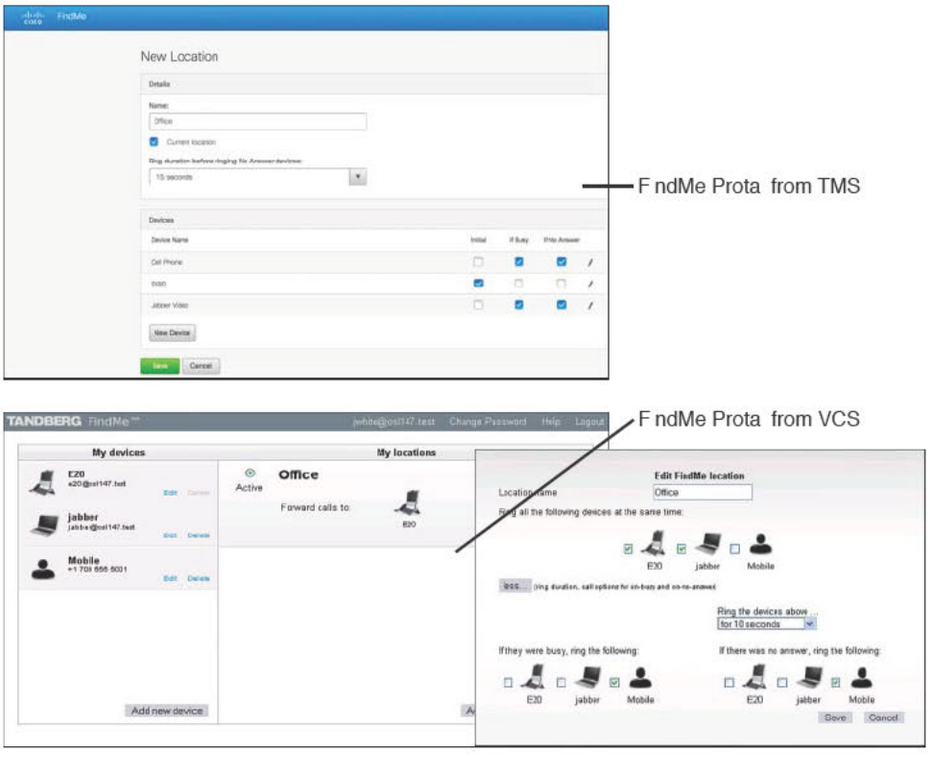


Figure 11-6 *FindMe User Portal on the VCS Compared to FindMe User Portal on TMS*

Notice in Figure 11-6 that none of the functions of the FindMe user portal has changed, only the skin of the user interface.

An important setting that must be configured on the VCS for clustering to work is a cluster name. Even if FindMe is used in a single VCS environment, it will not work until a cluster name has been created. User accounts are associated with the cluster name. So if the name is ever changed, those accounts will be lost unless they are reassociated with the new name. One other important consideration to configuring FindMe is that a user or administrator will want to add all the devices that could potentially be used in a FindMe environment before configuring the behavior. These devices could be any endpoint registered to the VCS, but could also include endpoints registered to the Cisco Unified CM, or even a Cisco Unity Voice Messaging account. Cisco Unified CM devices require a SIP trunk between the Cisco VCS and the Cisco Unified CM. Mobile phones, home land-line phones, and office ISDN phones can be added to FindMe as well, as long as an ISDN gateway or voice gateway exists within the network. Dial-plan considerations need to be taken into account when PSTN aliases are added to a FindMe account so that call transfer attempts can be sent to the gateway device.

Summary

It is said, "Invention is 10 percent sweat and 90 percent necessity." Networks have evolved significantly over the past three and a half decades. Much of the development in protocols and technologies has derived from needs that surfaced throughout this development process. Some of those needs have been addressed in this chapter, like the limitation of IPv4 that led to the development of IPv6 and NAT. NAT created other issues with communication across networks, specifically pertaining to voice and video over IP. The protocols that were developed by the IETF to overcome NAT traversal were STUN, TURN, and ICE. Although these protocols did resolve one issue, they simply bypassed a second issue: firewall traversal. A proprietary protocol came about, called Assent, that resolved both the NAT and firewall issues, and maintained a secure environment for corporate networks. The Assent protocol became the basis for the H.323 traversal standards of the ITU called H.460.17, H.460.18, and H.460.19.

All of these new standards and protocols led the way to the development of new technology products as well. Cisco has two call control solutions available for various industry needs, and there are also two traversal solutions that exist. For a Cisco VCS-centric environment, there is the VCS-traversal solution. This solution features the VCS Control and VCS Expressway as the traversal components needed. Within a Cisco Unified CM-centric environment, there is the collaboration edge solution. This solution features the Expressway Core and Expressway Edge as the traversal components needed. The Cisco Jabber Guest option offers an addendum to the collaboration edge solution. Cisco Jabber Guest allows businesses to extend their reachability to other businesses and customers who may not support a video communications solution.

Another technology developed over the years is call mobility. Cisco solutions offer two modes of accomplishing call mobility. In a Cisco Unified CM-centric environment, the Cisco Unified Mobility feature can be leveraged to allow employees to be contacted with a single number reach. In a Cisco VCS-centric environment, this is accomplished through a feature called FindMe.

Although the topics discussed in this chapter are beyond the scope of CIVND2, a basic understanding of them is expected by Cisco. This chapter has included more detail about these features and products to help prepare you with future certifications you may pursue, and to familiarize you with products and solutions being used in Cisco deployments globally.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 11-4 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 11-4 Key Topics for Chapter 11

Key Topic Element	Description	Page Number
Bullet Points	Identify the different private IP address classes and ranges.	252
Figure 11-1	Explain how STUN works.	254
Figure 11-2	Explain how TURN works.	254
Figure 11-3	Explain how ICE works.	255
Table 11-2	Identify the Assent and H.460.18/.19 ports needed for traversal.	256
Paragraph	Identify the components needed for a VCS-centric traversal solution.	257
Paragraph	Identify the components needed for a collaboration edge solution.	257
Paragraph	Explain what Mobile and Remote access is and how it works.	258
Table 11-3	Identify the different certification types used in Mobile and Remote access solution.	260
Paragraph	Explain the two Cisco call mobility options available.	263

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

IEEE, IETF, NAT, PAT, private Class A network, private Class B network, private Class C network, STUN, TURN, ICE, ICANN, TCP, UDP, DMZ, Assent, H.460.18/.19, PKI, Cisco Unified Mobility, FindMe

This chapter covers the following topics:

- **Collecting Logs and Status Information on Cisco TelePresence TC Software-Based Endpoints:** This section provides an overview of how to collect status and configuration information on TC software-based endpoints using the CLI, how to view current and historic log information from the web interface, and how to change the debug level on an endpoint to collect syslog information for SIP and H.323 calls.
- **Cisco TelePresence TC Software-Based Endpoint Maintenance:** This section examines how to back up the configuration settings on TC software-based endpoints and how to perform system upgrades.
- **Isolating and Identifying Issues on Cisco TelePresence TC Software-Based Endpoints:** This section examines how to isolate registration, call, and media issues on TC software-based endpoints.
- **Collecting Logs and Status Information on Cisco TelePresence CTS Software-Based Endpoints:** This section examines how to view log and call status information from the CTS software-based endpoint web interface.
- **Isolating and Identifying Issues on Cisco TelePresence CTS Software-Based Endpoints:** This section examines how to isolate registration, call, and media issues on CTS software-based endpoints.
- **Using the Cisco DX Series Problem Reporting Tool:** This section explains how to use the Problem and Reporting tool on DX series endpoints.
- **Isolating and Identifying Issues on Cisco Jabber Video for TelePresence:** This section examines how to isolate registration, call, and media issues on Cisco Jabber Video for TelePresence soft client.

CHAPTER 12

Operating and Troubleshooting Cisco TelePresence Endpoints

It is a wonderful, yet odd, feeling to install a Cisco TelePresence solution where everything works perfectly. It is an odd feeling because Cisco TelePresence endpoints are complex systems that involve many state-of-the-art peripherals for audio, video, and collaboration experience, and often the varying pieces and parts do not always work the way they are supposed to. Even after everything is installed and tested to working order, the human element will inevitably break something down the line, requiring someone to troubleshoot the issues at hand. This lesson will guide administrators to be proficient with various tools needed to operate and potentially troubleshoot these complex systems in a network environment.

This chapter describes the various tools that are used to perform regular tasks such as backup, restore, and performing upgrades. Other tasks described in this chapter include how to view call statistic information and pull logs to aid in troubleshooting Cisco TelePresence collaboration endpoints.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 12-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 12-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics	Questions
Collecting Logs and Status Information on Cisco TelePresence TC Software-Based Endpoints	1–2
Cisco TelePresence TC Software-Based Endpoint Maintenance	3–5
Isolating and Identifying Issues on Cisco TelePresence TC Software-Based Endpoints	6–7
Collecting Logs and Status Information on Cisco TelePresence CTS Software-Based Endpoints	8–9
Isolating and Identifying Issues on Cisco Jabber Video for TelePresence	10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. If an administrator were to issue the **debug** command on a TC software-based endpoint **log ctx sippacket debug**, what is the highest level debug that can be established?

   a. 6
   b. 9
   c. 12
   d. 15

2. How many historical log files can be stored on the Cisco TC software-based endpoint?

   a. 11
   b. 12
   c. 13
   d. 15

3. TC software-based endpoints can be backed up using which of the following options?

   a. OSD
   b. SCP
   c. FTP
   d. CLI

4. When upgrading a TC software-based endpoint, which of the following is required?

   a. Firmware packet
   b. Release key
   c. Option key
   d. Cisco Unified CM

5. Which of the following CLI commands can be used on TC software-based endpoints to verify IP connectivity to the VCS?

   a. **Utils Network Ping**
   b. **Utils Eth 0**
   c. **SystemTools Network Ping**
   d. **xCommand Ping**

6. If a technician is performing an integrated installation using a C60 endpoint, and an equalizer is introduced to handle ten microphones throughout the room, which of the following considerations needs to be taken into account?

   a. MIC settings on the endpoint need to be set to MIC level.
   b. MIC settings on the mixer need to be set to MIC level.
   c. MIC settings on the endpoint need to be set to Line level.
   d. MIC settings on the mixer need to be set to Line level.

7. How many DVI-I video inputs does a Cisco TelePresence codec C90 have?

   a. 1
   b. 2
   c. 3
   d. 4

8. Which log on the Cisco CTS software-based endpoints shows SDP messages?

   a. Sysop Log
   b. Log Files
   c. SIP Messages
   d. System Status

9. Which of the following CLI commands can be used on CTS software-based endpoints to verify IP connectivity to the Cisco Unified CM?

   a. **Utils Network Ping**
   b. **Utils Eth 0**
   c. **SystemTools Network Ping**
   d. **xCommand Ping**

10. What is the minimum bandwidth rate a Cisco Jabber Video for TelePresence call can make during a video call?

    a. 384 kbps
    b. 128 kbps
    c. 64 kbps
    d. 24 kbps

Foundation Topics

Collecting Logs and Status Information on Cisco TelePresence TC Software-Based Endpoints

Chapter 10, "Configuring Cisco TelePresence TC Software-Based Endpoints," described the various user interfaces on the Cisco TelePresence TC software-based endpoints. These interfaces can be used to verify the status of TC endpoints and to collect logs. The onscreen display can be used to display the System Information screen, which provides network, endpoint registration, and current call details. The General section shows the software version, system IP address, MAC address, serial number, and licensing information. From the web interface, you can display basic system information and registration information on the Home page. You can display call statistics from the Call Control page. The i button will display call statistic information, such as the protocol being used, audio and video codecs, bandwidth rates, and all based on send and receive directions. You can retrieve various system event logs from the web interface, and use the command-line interface (CLI) to set up the log level from less to more verbose. In addition, you can use the CLI from the serial line, Secure Shell (SSH), or Telnet to display the network status and information about the endpoint hardware and software and perform endpoint diagnostics. For endpoint monitoring and troubleshooting, the CLI is the most powerful interface, compared to other user interface options.

Three CLI **status** commands prove very useful when troubleshooting endpoints. The **xStatus H.323** and the **xStatus SIP Profile 1** commands show registration details about the endpoint for H.323 and Session Initiation Protocol (SIP). The command **xStatus Call** shows call statistic information. Whenever you escalate system issues to Cisco Technical Assistance Center (TAC), include this generated system information with the ticket. Other useful commands include **xConfiguration** and **xStatus Network 1**.

Cisco TC software-based endpoints can be set up to provide H.323 and SIP debug log information. You can access the collected information from the web interface by navigating to the **Diagnostics > Log Files** menu. Debug information is stored in the Eventlog/application.log file. Clicking this file will open it in Text format. If the information is distorted, try copying and pasting the information into a document reader that understands Extensible Markup Language (XML) format, like Microsoft Word.

A different command enables debug for H.323 and SIP. There is also a command that will enable a Real-time Transport Protocol (RTP) statistics debug. To enable debug and set the logging level, log in to the CLI as the admin user. Depending on the signaling protocol, enter one of these commands:

- **log ctx H323packet debug 9**
- **log ctx SipPacket debug 9**
- **log ctx RTPstatistics debug 3**

Debug collects call setup information. Make a call between the endpoint debug was turned on for and another endpoint. Always try to collect call setup and call teardown

information. If this information is collected to troubleshoot an issue other than something related to call setup or call teardown, also try re-creating the issue. Once the call is torn down, it is important to turn off debug on the endpoint. This can be accomplished two ways. When the endpoint is rebooted, all debug information is torn down. However, the log information collected is compressed into a zip folder, making it harder to retrieve. If the desired outcome is to view the information immediately after collecting it, the **debug off** commands need to be used. Enter one of these commands to turn off debug:

- **log ctx H323packet debug off**
- **log ctx SipPacket debug off**

Leaving SIP or H.323 logs running may fill up the hard disk and the endpoint might crash or reboot. The Eventlog/application.log file is limited to 1 MB only. This storage space holds approximately 18 minutes of logging before the call log is wrapped and started all over again.

The Eventlog/application.log file contains many events that are related to the call and to the endpoint system in general. Understanding an H.323 or SIP call process is critical to being able to read and understand the debug information captured in the Eventlog/application.log file. In an example with SIP, Early Offer is most commonly used. The SIP call process starts with an Invite message, within which the source endpoint also sends the Session Description Protocol (SDP) communication. The receiving endpoint responds with a Ringing and OK message, sending its own SDP response. These messages are the key elements you need to look for to follow the call setup flow. Example 12-1 illustrates a SIP syslog captured on a TC endpoint using the previous **debug** command.

Example 12-1 *SIP Syslog on a TC Software-Based Endpoint*

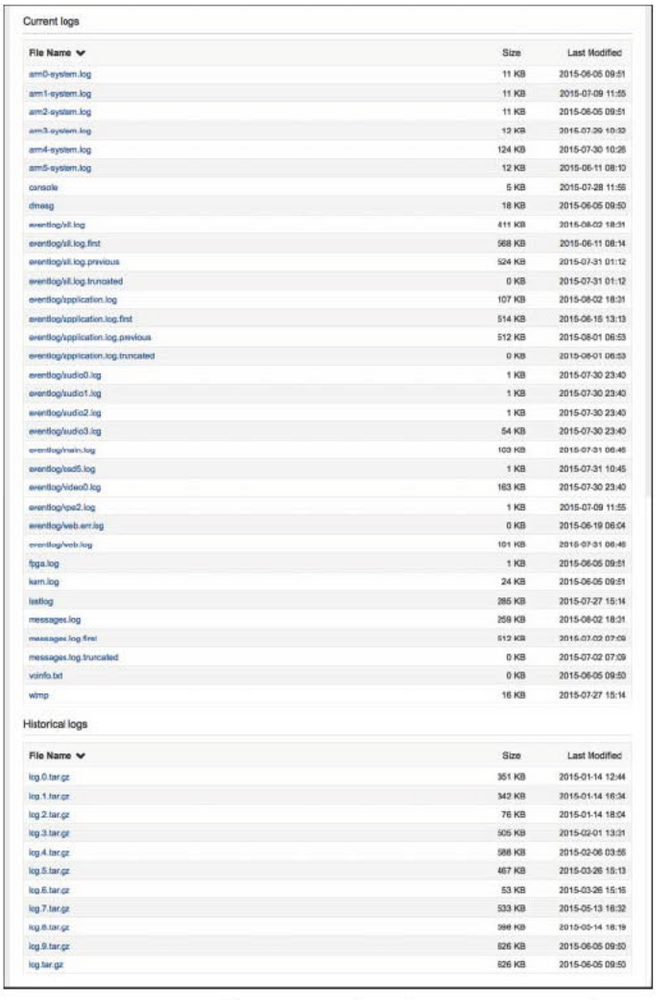
```
INVITE sip:lv03@compass.com SIP/2.0
   Via: SIP/2.0/TCP 192.168.192.101:5060;branch=z9hG4bK56020e13ce61a5d27e82a45e3632999
0.1;rport
   Call-ID: f61192638f720f280ccda079cc4189be
   CSeq: 100 INVITE
   Contact: <sip:419211@compass.com;gr=urn:uuid:f15a8055-526a-5217-8774-eac257949b7d>
   From: <sip:419211@compass.com>;tag=da4cc2ead6588782
   To: <sip:lv03@compass.com>
   Max-Forwardszzzzzz: 70
   Route: <sip:192.168.192.40;lr>
   Allow: INVITE,ACK,CANCEL,BYE,UPDATE,INFO,OPTIONS,REFER,NOTIFY
   User-Agent: TANDBERG/519 (TC7.0.2.aecf2d9)
   Supported: replaces,100rel,timer,gruu,path,outbound,sdp-anat
   Session-Expires: 1800
   Content-Type: application/sdp
   Content-Length: 2756

   v=0
   o=tandberg 94 1 IN IP4 192.168.192.101
   s=-
```

```
    c=IN IP4 192.168.192.101
    b=AS:1920
    t=0 0
    m=audio 16732 RTP/AVP 107 108 109 110 104 105 9 18 8 0 101
    b=TIAS:128000
    a=rtpmap:107 MP4A-LATM/90000
    a=fmtp:107 profile-level-id=25;object=23;bitrate=128000
    a=rtpmap:108 MP4A-LATM/90000
m=video 16734 RTP/AVP 97 126 96 34 31
    b=TIAS:1920000
    a=rtpmap:97 H264/90000
    a=fmtp:97 packetization-mode=0;profile-level-id=428016;max-
br=5000;max-mbps=108000;max-fs=3600;max-smbps=108000;max-fps=6000;max-
rcmd-nalu-size=1382400
    a=rtpmap:126 H264/90000
m=application 29499 UDP/BFCP *
m=application 16738 RTP/AVP 100
    a=rtpmap:100 H224/4800
```

A few key elements are highlighted. Notice the Invite message starting the communication, followed by the alias dialed. The IP address and source alias are also provided in the opening packets sent. Reading down a little bit is the SDP message. The V=0 line marks the beginning of the actual SDP session. The next significant marker to look for is the m=. This marks the media capabilities of the source endpoint, listed in the order it wants to use them. The first media capabilities listed will always be audio. 16732 is the RTP port the source endpoint wants to use. RTP ports are always even in number. It can be assumed that the RTP Control Protocol (RTCP) port will be the previous odd number in sequential order. AVP stands for Attribute-Value Pair and is followed by SIP cause codes for audio codecs. These cause codes do not need to be memorized because the next lines in a SIP syslog are the attributes of the cause codes. Notice in Example 12-1 that cause code 107 refers to MP4A-LATM. This is an advanced Internet audio codec developed in 1997 by Bell Labs, Fraunhofer Institute, Dolby Labs, Sony, and Nokia. Similar to the audio media, next you will find m=video for the video media specifications. There are also lines for BFCP (Binary Floor Control Protocol) and H.224 FECC (Far-End Camera Control). If the second m=video line is not present, it means that this call is an audio only call, whether that was the intent of either participant or not. This could help lead to troubleshooting issues for video calls that do not stream video. Next, you would see the Ringing message followed by the SDP exchange from the destination endpoint, and so on until the call is set up. H.323 statistics can also be pulled using this same process. The call setup for H.323 calls could be followed in a similar fashion.

TC software-based endpoints continuously collect other information about various system parts and store that information in the log files accessed by the web interface. Using the web interface, navigate to **Diagnostics > Log Files**. The Current Logs section shows all information that has been logged since the last system reboot. The current event log files are uncompressed. Once an endpoint is rebooted, all the Current Log information is compressed and stored in a Historical Logs file. The Historical Logs contain 11 different

zipped files. Immediately after a reboot, the Current Logs information is stored as log.tar.gz. During the next system reboot, log.tar.gz becomes log file log.tar.gz.(0-9). Once a log.tar.gz file is moved to a numeric placeholder, it remains there until it is the oldest log file, at which time it is deleted. Figure 12-1 illustrates how the current and historical logs appear in a TC software-based endpoint.



Current logs

File Name	Size	Last Modified
arm0-system.log	11 KB	2015-06-05 09:51
arm1-system.log	11 KB	2015-07-09 11:55
arm2-system.log	11 KB	2015-06-05 09:51
arm3-system.log	12 KB	2015-07-30 10:33
arm4-system.log	124 KB	2015-07-30 10:26
arm5-system.log	12 KB	2015-06-11 08:10
console	5 KB	2015-07-28 11:55
dmesg	18 KB	2015-06-05 09:50
eventlog/sll.log	411 KB	2015-08-02 18:31
eventlog/sll.log.first	568 KB	2015-06-11 08:14
eventlog/sll.log.previous	524 KB	2015-07-31 01:12
eventlog/sll.log.truncated	0 KB	2015-07-31 01:12
eventlog/sppication.log	107 KB	2015-08-02 18:31
eventlog/sppication.log.first	514 KB	2015-06-15 13:13
eventlog/sppication.log.previous	512 KB	2015-08-01 06:53
eventlog/sppication.log.truncated	0 KB	2015-08-01 06:53
eventlog/sudio0.log	1 KB	2015-07-30 23:40
eventlog/sudio1.log	1 KB	2015-07-30 23:40
eventlog/sudio2.log	1 KB	2015-07-30 23:40
eventlog/sudio3.log	54 KB	2015-07-30 23:40
eventlog/swin.log	103 KB	2015-07-31 06:46
eventlog/sxd5.log	1 KB	2015-07-31 10:45
eventlog/video0.log	183 KB	2015-07-30 23:40
eventlog/vpe2.log	1 KB	2015-07-09 11:55
eventlog/web.err.log	0 KB	2015-06-19 06:04
eventlog/web.log	101 KB	2015-07-31 06:46
fpga.log	1 KB	2015-06-05 09:51
kern.log	24 KB	2015-06-05 09:51
lastlog	285 KB	2015-07-27 15:14
messages.log	259 KB	2015-08-02 18:31
messages.log.first	512 KB	2015-07-02 07:09
messages.log.truncated	0 KB	2015-07-02 07:09
vsinfo.txt	0 KB	2015-06-05 09:50
wmp	16 KB	2015-07-27 15:14

Historical logs

File Name	Size	Last Modified
log.0.tar.gz	351 KB	2015-01-14 12:44
log.1.tar.gz	342 KB	2015-01-14 18:34
log.2.tar.gz	76 KB	2015-01-14 18:04
log.3.tar.gz	505 KB	2015-02-01 13:31
log.4.tar.gz	588 KB	2015-02-06 03:55
log.5.tar.gz	467 KB	2015-03-26 15:13
log.6.tar.gz	53 KB	2015-03-26 15:15
log.7.tar.gz	533 KB	2015-05-13 18:32
log.8.tar.gz	398 KB	2015-05-14 18:19
log.9.tar.gz	826 KB	2015-06-05 09:50
log.tar.gz	826 KB	2015-06-05 09:50

Figure 12-1 *TC Software-Based Endpoint Current and Historical Logs*

12

Cisco TelePresence TC Software-Based Endpoint Maintenance

Key Topic

Cisco TelePresence TC software-based endpoints provide two options natively for creating a system backup. The first option involves amassing the output data of the configuration settings through the CLI. The second method is a new feature that enables an administrator

to perform a backup using the web interface. Backups should always be performed when the endpoint has a known working configuration and before performing a system upgrade. The text that follows describes how to perform a backup using both methods.

Backing up a Cisco TC software-based endpoint through the CLI is a good method to use if an administrator ever needs to modify the configuration settings before performing a system restore. To perform a backup using the CLI, log in to the system as admin using SSH or Telnet. Make sure that the terminal emulation software that you are using can capture and save the output data to a text file. To collect the system configuration settings, execute the **xconfiguration** command. This issues a copy of all the configuration settings available with the parameters to which they are already set. Close the terminal session when completed and open the text file that was created. The star c space denoted as follows (*c) at the front of each line indicates that line is a copy of the **xConfiguration** command. They will all need to be deleted. The Find/Replace tool is the easiest way to delete these characters. Also, delete any other information that is not part of an **xConfiguration** command. Save the text file after completing these changes because this is your backup. You can also use the CLI to upload this file to the Cisco TelePresence TC software-based endpoints when you need to restore the configuration. Simply copy the data in the text file and paste it into a new CLI session. A system reboot may be required after the restore if the system IP settings change. If they do not change, a system reboot is not required.

Another method used to back up the system configuration is to use the web interface. Navigate to **Maintenance > Backup and Restore**. Click the **Take Backup** button. A copy of the system configurations will be saved to your computer. To restore these settings, browse and select the backup you took from the web interface, and then click **Restore**. Alternatively, the backup taken through the CLI can be restored using the web interface restore tool. Whichever method is used to back up the endpoint, it is important to note that a backup only backs up the configuration files. It does not back up licenses or option keys.

The way to perform a TC software-based endpoint upgrade has changed over the years since TC1.0 first came out. There have been two things required to upgrade these endpoints from Version 1 to Version 6. An administrator was required to have the firmware packet and a release key before major firmware upgrades could be performed. However, after an administrator upgrades an endpoint to version TC6.1, the release key is no longer needed to perform major upgrades. It is assumed that Cisco no longer requires a release key so that updated firmware can be pushed from the Cisco Unified CM; however, at the time of this writing, the Cisco Unified Communications Manager (CM) cannot upgrade the firmware on TC software-based endpoints yet.

Native on the endpoint, all TC software-based endpoint software upgrades and option keys are managed from the web interface. To upgrade the system software, you must first download the package file from the Cisco software repository. The filename looks similar to s52000tc7_1_1.pkg or s52010tc7_1_1.pkg, where 7_1_1 denotes software version 7.1.1. After the package file has been downloaded, log in to the web interface of the endpoint as admin and navigate to **Maintenance > Software Upgrade**. Click **Browse** and choose the

package file you downloaded from Cisco. Click **Upgrade**. The system starts downloading the file to the endpoint's local disk and then performs the upgrade from that disk. Do not use the endpoint during the upgrade; doing so might interrupt the process. The endpoint reboots twice during the upgrade. The first reboot is used to finalize the endpoint upgrade. The second reboot is to finalize the camera upgrade. When the upgrade is successfully completed, a message appears. This process can take up to 30 minutes.

On the same upgrade page of the web interface, an administrator can add option keys for new features as required. Option keys allow for extended functionality of the system and do not require a reboot when added. You might have several option keys in your system. Review Chapter 7, "Cisco TelePresence Endpoint Characteristics," for information about available TC software-based endpoint option keys. If you need to downgrade the software on Cisco TelePresence TC software-based endpoints, you may need to open a Cisco TAC case to obtain special release keys.

There is another option to back up, restore, and upgrade TC software-based endpoints. Cisco TelePresence Management Suite (TMS) is a complete management tool that enables administrators to manage an entire video network from a single interface. Be aware that backups cannot be scheduled, nor should they be. Consider if an endpoint were scheduled to be backed up by TMS and someone changed settings on that endpoint before the backup took place; in this case, issues relevant to those changes would be backed up as well. However, using TMS to perform these tasks offers many benefits. Though a backup cannot be scheduled, a restore can be. After endpoints have been backed up, an administrator can schedule that those endpoints are restored once a day or once a week. Two of the main benefits of using TMS for upgrades are the ability to perform bulk upgrades with a single click of a button and upgrades can also be scheduled to occur at a time when the systems will not be in use, such as on a Saturday at midnight. The subject of how to use TMS to perform these tasks is beyond the scope of the Cisco CIVND material. However, further discussion on Cisco TMS will follow in later chapters.

Isolating and Identifying Issues on Cisco TelePresence TC Software-Based Endpoints

Troubleshooting issues on Cisco TelePresence TC software-based endpoints can be a particularly cumbersome task because the call control mechanism used could be the Video Communication Server (VCS), which supports H.323 and SIP, or it could be the Cisco Unified CM with SIP. The tools used for troubleshooting may depend on the issue type being experienced or the type of issue needing fixed. There are different tools available for troubleshooting registration issues, call setup issues, or media issues. The web interface, onscreen display, and the CLI provide call statistics that include packet loss, jitter, and delay statistics for incoming and outgoing audio and video channels. Figure 12-2 illustrates what the call statistics look like during a video call on an SX10 endpoint.

Audio	Transmit	Receive
Protocol	AACLD	-
Resolution		
Frame rate		
Channel rate	63 kbps	-
Total packet loss	0.0%	0.0%
Current packet loss	0.0%	-
Jitter	2 ms	3 ms
Video	Transmit	Receive
Protocol	H264	H264
Resolution	768x448	320x240
Frame rate	30 fps	16 fps
Channel rate	318 kbps	144 kbps
Total packet loss	0.0%	0.0%
Current packet loss	0.0%	0.0%
Jitter	2 ms	6 ms

Figure 12-2 *Call Statistics from an SX10 Endpoint*

Jitter is the variation of delay between packets received by the endpoint. To check for packet loss in a call, check the system information screen or use the **xStatus Diagnostics** command. Using this command, you can see the same output information that this figure shows. The main areas of packet loss will probably be on the video channels, but can also be on the audio. Dropped packets are packets that arrive too late to be used or that were lost and never received. You can also see the jitter statistics and the channel rate. The video channel rate can change dynamically, depending on how much change is in the picture. If there is excessive packet loss or high jitter, you need to look at the network to determine the cause or escalate the issue to the network team.

Key Topic

Many of the tools used to troubleshoot registration issues depend on which call control model the endpoint uses. However, a good place to begin troubleshooting registration issues in either call control scenario is with IP connectivity issues. There are tools built in to the CLI of TC software-based endpoints that can aid in verifying network connectivity issues. The CLI command **SystemTools Network Ping** followed by the IP address of the Cisco VCS or Cisco Unified CM is one of the commands that you can use. Another command is **SystemTools Network TraceRoute** followed by an IP address. This second command will not only test network connectivity, but will also verify the route taken to connect the endpoint to the destination IP address and the number of hops it took to reach that destination. The command that enables you to verify that the network processes are running and listening on the correct protocol ports is **SystemTools Network Netstat**.

If IP connectivity were working across the network, the next step to troubleshooting registration issues on TC software-based endpoints would be to look for nonmatching configuration settings between the server and the endpoint. For Cisco VCS registration issues, you need to make sure that the protocol that is used (H.323 or SIP) is enabled at both the endpoint and the server. With H.323, calls are possible without registering to a gatekeeper if the call setup mode is set to **Direct**. In direct mode, the endpoint never tries to register to a gatekeeper. If the desired outcome is for the endpoint to register to the VCS, the call setup mode will need to be set to **Gatekeeper**. In gatekeeper mode, calls are not possible until the endpoint registers. The discovery mode on the Cisco VCS determines how the endpoint will try to discover the call control server for both H.323 and SIP. If the discovery mode is set to **Automatic**, the TC software-based endpoint sends out a broadcast request searching for any call control device to which it can register. The first call control server to respond is where the endpoint will try to register, which may not be where the administrator intended the endpoint to register. If there is no response, registration fails. Best practice suggests setting the discovery mode to **Manual** and entering the specific address of a call control server to which the endpoint will try to register. H.323 registration requests always use UDP port 1719 for Registration Request (RRQ) messaging to a gatekeeper. SIP, however, could use UDP port 5060 or UDP over TLS 5061. Make sure that the correct matching transport protocol is set at both the endpoint and the server for SIP. Note that discovery mode has no bearing on TC software-based endpoint registration to the Cisco Unified CM.

Issues registering to the Cisco Unified CM are typically caused because the voice VLAN was not learned from the switch, Dynamic Host Configuration Protocol (DHCP) did not provide the correct IP settings or the right TFTP server address through Option 150, IP connectivity to the Cisco Unified CM server or Cisco TFTP server is broken, or the endpoint is provisioned incorrectly. This is also true for Cisco TC software-based endpoints trying to register to the Cisco Unified CM. Verify that external manager mode is set to **CUCM**. If you configure the Cisco TFTP server IP address manually, verify that the correct address is set in the Cisco TelePresence TC software-based endpoint External Manager Address field. Also verify that HTTP is chosen for the external manager in the advanced settings configuration.

Provided the endpoint has registered to the call control server, the next issue that could be encountered relates to call setup. Because of the complexity of the setup, a great variety of problems can be experienced when setting up a call with a Cisco TelePresence TC software-based endpoint. There are few tools on the endpoint itself that can help detect call setup issues. Most of the tools reside in the Cisco Unified CM or the Cisco VCS, which are beyond the scope of this class. Verify that the dial plan is correct and that calls can be successfully routed by using it. Take a screen capture of system configuration settings, status messages, and debug files, and then escalate call setup issues to a call control administrator. These administrators can verify CAC settings used to set up bandwidth limits and call privileges that can accommodate a certain number of calls.

Media issues can be as complex as call setup issues to troubleshoot because many moving parts can impact audio and video packets sent and received. Video input devices include cameras, computers for content sharing, document cameras, and video-playing devices.

Video output devices include monitors and projectors. Audio input devices include microphones and possibly mixers. Audio output devices include speakers and amplifiers. The speakers can be freestanding, ceiling mounted, or embedded in monitors. Plus, the cables and connectors present their own limitations, not to mention the impact network connections can have on the quality of media between two devices when connected in a call. Administrators can use the **xStatus media channels** command from the CLI to help isolate media issues. Table 12-2 illustrates some of the components that could impact media quality issues.

Key Topic

Table 12-2 Audio and Video Components

Audio Input Devices	Audio Output Devices	Video Input Devices	Video Output Devices
Microphones (MIC level)	Speakers (free standing)	Cameras	TVs
Microphones (Line level)	Active amplifiers	Computers	Monitors
Mixers	Passive amplifiers	Document camera	Projectors
Echo cancellation	Speakers (built in to monitor)	Video-playback Device (DVR, DVD, Blu-ray)	

Packet loss results in a poor user experience and can usually be seen by artifacts on the screen. Administrators can check call statistics to see whether the network is experiencing packet loss. If the user cannot see incoming video, the video output port being configured incorrectly could cause this, or a resolution being set that the monitor does not support. A special sequence on the remote control can fix this problem. Press the remote control keys in the following sequence: **Disconnect * # * # 0** *X* **#** (where *X* is the video output of the monitor in which you want to display). You can also use the CLI command **xConfiguration Video OSD Output: <1-4>** to set the onscreen display output to the relevant video output source. Either of these options changes the onscreen display (OSD) port and sets the resolution to **auto detect**. If a monitor displays an image outside of the monitor frame, be aware that most monitors will overscan TV resolutions such as 720p and 1080p. Use the monitor menus to fix overscan settings. Alternatively, you can use the Endpoint Administrator Settings menu to change the video-output resolution. To check or change the video-output resolution, navigate to **Configuration > System Configuration > Video > Output, HDMI 1 > Resolution**. If you are using a TV as an external monitor, it is recommended to change the settings of the TV to gaming mode to reduce latency. Because High-Definition Multimedia Interface (HDMI) cables do have different quality ratings, it is also recommended to use a good-quality HDMI cable over lengths no more than 15 meters.

Multiple video input sources can be used to daisy chain cameras together. Only control is being daisy chained between the cameras using the Video System Control Architecture (VISCA) cascading cable; therefore, each camera must have a physical connection back to the codec. This connection could use different connector types; therefore, each input

port on a TC software-based endpoint supports varying different connectors. Only one connecter for each port can be active at a time. For example, the Cisco TelePresence codec C90 allows you to connect a maximum of 12 high-definition video input sources, but only 5 can be active simultaneously. Table 12-3 illustrates the video input ports available on the Cisco TelePresence codec C90. This information is also available on the back of the endpoint itself.

Key Topic

Table 12-3 Cisco TelePresence Codec C90 Video Input Ports

Video Input 1	Video Input 2	Video Input 3	Video Input 4	Video Input 5
HDMI 1	HDMI 2	HDMI 3	HDMI 4	HDMI 5
HD-SDI 1	HD-SDI 2	HD-SDI 3	HD-SDI 4	Composite 5
YPrPb 1	YPrPb 2	DVI 3	-	YC 5

Based on an understanding of the preceding information, if an endpoint is not able to send video in an environment that supports multiple cameras daisy chained together, this could be corrected by changing the video input port. When you install but cannot control a second Cisco TelePresence PrecisionHD 1080p camera on your TC software-based endpoint codec, ensure that a VISCA cascading cable is being used to connect the cameras, and that the appropriate video-input source is set to which camera you should control when this particular video-input source is active.

If you cannot get any audio from the codec when it is connected to the monitor by using HDMI, check whether the video output resolution for HDMI 1 is set to 800x600 or 1900x1200. These two resolutions run in DVI mode (DVI over HDMI), which does not support audio. If the audio on the dual stream is out of sync with the dual-stream video, be aware that lip synchronization is not supported over SIP. If audio is distorted, one of these issues might be the cause. Echo cancellation is not working and might be disabled. HDMI is being used for audio, but the audio is delayed by processing on the monitor. Modern TVs are often used and have picture processing that can delay the audio, and the codecs cannot echo-cancel this situation. Determine whether the monitor has a game mode or other nonprocessing mode to stop any video and audio processing. You can test whether the monitor is the issue by attaching some active speakers to the codec output and determining whether there are still echo-cancellation issues. Echo cancellation on Cisco TelePresence TC software-based endpoints supports a maximum of 340 ms on all the audio bandwidth.

Collecting Logs and Status Information on Cisco TelePresence CTS Software-Based Endpoints

Key Topic

Cisco CTS software-based endpoints do not have as many loggings and troubleshooting features available native on the endpoint as Cisco TC software-based endpoints. However, there are some logs available that can be used to help isolate problems when they occur. These logs are accessed through the Cisco CTS web interface. Selecting the **Troubleshooting** menu option on the left column offers three tabs with different logging options. They are Sysop Log, Log Files, and SIP Messages.

The Sysop Log tab displays system operation messages, including call information, call statistics, and call errors for the Cisco TelePresence System. As many as 20 individual files are saved on the Cisco TelePresence System, and each file can contain as many as 100,000 characters. To download the log files, click the **Download Sysop Files** button at the bottom of the page. The prompt that comes up presents two options: open to view the log files or save the log files to the local disk on your computer. If the option to open the log file is chosen, the last 100,000 bytes of the log are shown, and all available systems operation log files are downloaded.

The Log Files tab allows administrators to download log files or capture new log files. You can choose from three download options by selecting the appropriate radio buttons. None is the default, and no log files are captured unless a download option is chosen. The Download Existing Log Files option allows you to download existing log files. Click this radio button and then choose a problem from the Select Problem Type drop-down list to download logs. The drop-down list contains the following problem types: Audio (Speakers, Microphones), Video (Displays, Cameras), Projector, LCD, Document Camera, Phone, Recording, and Other/Unknown. When you click **Download Existing Log Files**, the system shows the message "A WinZip download will start within several minutes. Please wait." The File Download window appears, prompting you to open or save the file. The other option available within the Log Files tab is to Capture New Log Files. After you choose from the Select Problem Type drop-down list and click **Capture New Log Files**, the system displays the message "Collecting Cisco TelePresence System log files. This process may take several minutes. Please wait." The File Download window appears, prompting you to open or save the file. When you capture new log files, the system combines and compresses all existing log files from the codec. The Log Files tab displays the status of the log capture, including the percentage of completion.

The SIP Messages tab displays all SIP messages sent and received by the CTS software-based endpoint. You can filter the SIP messages to display a specific type of message in the SIP log file. You can also choose the number of messages to view at one time. Double-clicking a SIP message from the list opens the SIP Message Details dialog box for detailed message reports. You can do the same thing by highlighting the SIP message and clicking **Details**.

Viewing real-time call statistics is an important function on any endpoint. From the Cisco CTS web interface, choose **Monitoring > Call Statistics**. The Real Time Call Statistics section lists the details of an in-progress call, including the connection status, registration status, and local directory number. There is also a Historical Call Statistics (Not Including Current Call, If Any) section that lists historical information about past calls. There are also Audio/Video Call sections that list details about a call, such as audio stream statistics of an audio/video call, video stream statistics of an audio/video call, and audio-only call stream statistics. These call statistics show both transmit and receive call information. Other critical information displayed includes local and remote endpoint IP address information, average latency, differentiated services code point (DSCP), and class of service (CoS) quality of service (QoS) markings.

Isolating and Identifying Issues on Cisco TelePresence CTS Software-Based Endpoints

Troubleshooting issues on Cisco CTS software-based endpoints is very similar to troubleshooting collaboration endpoints in a Cisco Unified CM environment because the registration and call processes are the same. Knowing the registration process is important to understanding the process of troubleshooting registration issues because those processes are two in the same. The CTS software-based endpoint must first obtain power from the power cube and load its locally stored image file. Then the endpoint sends out a Cisco Discovery Protocol (CDP) request for VLAN and QoS information from the switch. Once that information is obtained, the endpoint must reach out to the DHCP server for assignment of an IP address, subnet mask, default gateway address, and optionally the TFTP server address through Option 150. After the TFTP server address has been identified, the endpoint sends a TFTP Get message to the TFTP server for configuration information, providing its MAC address as identification. Based on the MAC address provided, the TFTP server provides all the configuration settings the endpoint needs for registration and updated firmware load files, if needed. After the endpoint receives this information, provided it does not need to upgrade and reboot, it sends a SIP registration request to the Cisco Unified CM. When the Cisco Unified CM responds with a SIP OK message, the CTS software-based endpoint is registered. If the endpoint does not register, begin troubleshooting by examining each of these steps until the issue has been isolated to a single step. Resolve the issue and re-initiate the registration process again by rebooting the endpoint.

Working through each of these steps in order, an administrator should first examine the CDP process. A Cisco CTS software-based endpoint must either obtain voice VLAN from the switch via Cisco Discovery Protocol or manually configure the VLAN. The switch might be incapable of CDP, or the CDP service might not be running on the Cisco CTS endpoint. You can verify whether the process is running by using the CLI command **utils service list**.

If VLAN settings were correct on the Cisco CTS endpoint, the next item to check is the IP settings. Typically, all IP parameters are obtained using DHCP. If the DHCP server is unreachable or runs out of IP addresses, the endpoint will be unable to communicate across the network. This often occurs when the Cisco Unified CM is used as the DHCP server because it can only lease up to 1000 IP addresses. In cases where CTS software-based endpoints do not receive a DHCP address, the endpoint displays the default IP address 192.168.100.2 during the boot process. This address can be used to statically assign an IP address to the endpoint through the web interface, which can aid in troubleshooting network-related issues. Provided no network issues are apparent, there might be an issue with IP routing to or from the Cisco Unified CM cluster. You can use the CLI to verify IP settings and perform diagnostics. Use the **show network eth0** command to display the current IP settings, connectivity to the switch, and VLAN. Use the **utils network ping** command to discover whether there is IP connectivity to the server. If you suspect IP routing problems, you can use the **utils network tracert** command to discover the section of the network that has the IP routing issue. You can also use the **show network status** command to display all processes and their associated port numbers and existing socket connections. If your network uses DNS, you must verify that the server names are properly resolved to IP addresses. A firewall can also introduce reachability problems when it filters the traffic

that is required for successful registration, such as SIP and HTTP traffic. Make sure that the UDP and TCP SIP ports 5060 and TCP HTTP port 6970 are open.

If there were no network-related issues found, the next step an administrator must examine is whether the endpoint has obtained the appropriate IP address of the Cisco TFTP server. This IP address is usually obtained through Option 150, although it can be configured manually. The Cisco Unified CM cluster might also be causing issues if the endpoint is not configured and automatic provisioning is disabled or if required services are not responding.

Oftentimes, CTS software-based endpoints show as registered to the Cisco Unified CM, but the touch panel does not work. This issue is usually due to the panel-to-system communication. The touch panel automatically obtains its IP address from the endpoint built-in DHCP server. Make sure that the server process runs normally using the CLI command **utils service list**. When you display the system status at the touch panel, the panel should show the correct IP address. Another issue that could prevent the touch panel from functioning properly is related to the firmware load file. When the CTS endpoint receives firmware bin files from the TFTP server some of the bin files contain the firmware for the touch panel, which the CTS endpoint is responsible for delivering. If the endpoint performs an upgrade during the registration process, something could have prevented the CTS endpoint from delivering the appropriate files to the touch panel. Try rebooting the endpoint to reinitiate this process. If that does not work, check that the Cisco Unified CM has the appropriate files upload for the version the CTS endpoint is running. There should be three files listed (two for the CTS endpoint, and one for the touch panel).

If you experience degraded audio quality or the call is dropped completely, the Cisco TelePresence endpoint might be experiencing packet loss or packet jitter for an extended period. Verify packet loss and jitter through system operation logs or live call statistics from the CLI or web graphical user interface (GUI). Check the network path to determine whether jitter or packet loss is observed. If users experience choppy audio during bidirectional discussions, the issue might be caused when the audio echo canceller briefly mistakes one of the speech patterns for noise and cancels it, resulting in choppy audio. The audio from the remote side is slightly attenuated before being played out to the speaker. The echo-cancellation feature removes some of the sound from the talkers during the bidirectional discussions. Check whether there has been a change in the echo path. For example, someone may have moved the speakers or microphone, or there could be a laptop or other device directly placed in front of the microphone. Otherwise, this behavior is expected. The existing filter parameters should be enough to cancel the sound from the speaker. However, during bidirectional discussions, echo cancellation always removes some sound from the talker. High CPU or resource saturation can cause hearing echo. This situation might cause audio-missed interrupts on the endpoint. To get rid of the echo, you can perform a hold or resume of the call or redial it completely. When you hear echo, the most common issue is the room acoustic environment. Rarely, the issue is an audio port or microphone issue. To mitigate the issue, you can install an acoustic panel, or you can put in some furniture or plants and make sure that the audio volume is set to medium. Check the microphone and audio port. Unplug or mute the suspected microphone. If the problem persists, the microphone or that audio port is probably the issue. Swap the microphone for another one and see whether the problem follows the microphone or the codec. Plug only one microphone into an audio port at a time and continue through all the microphones and audio ports to

isolate the problem. Another cause for media issues on any endpoint has to do with duplex. Video endpoints must use full duplex. Check that the switch ports, endpoints are connected to and ensure they are not using half duplex. In most cases, autonegotiation will result in full duplex being used, but this is not always true, which is why it is always good to check.

Using the Cisco DX Series Problem Reporting Tool

The Cisco DX650 includes an integrated Problem Report Tool to provide support for device-related issues. To access the tool, choose **Settings > About Device**. The first page provides information about the endpoint including the model number, Android version, kernel version, and build number. When you scroll to the second page, the information displayed includes the active load, last upgrade, active server, and standby server. To report a problem to Cisco, choose **Cisco Collaboration Problem Reporting Tool**.

Users can issue a notification from the device by providing the following information:

- Select the date that the problem was observed. This field is autopopulated with the date the tool was invoked, but it can be changed if needed.
- Select the time that the problem was observed. This field is also autopopulated with the time the tool was invoked and can be changed.
- Select the problem application. If you are unsure of the application that had the problem, choose **None**.
- Enter a problem description. Include a concise description of the behavior that was observed.
- Enter a customer support e-mail address.

Tap **Create Problem Report** when finished.

Isolating and Identifying Issues on Cisco Jabber Video for TelePresence

The best tools available to aid in troubleshooting Cisco Jabber Video for TelePresence are the Cisco VCS and Cisco TMS because they completely control the Jabber Video for TelePresence client. The means of using the VCS and TMS for troubleshooting goes beyond the scope of the Cisco CIVND2 course; however, Cisco Jabber Video for TelePresence does provide error logging that can be used during the troubleshooting process when registration issues are experienced. Before these logs are used to troubleshoot registration issues, the following information should be verified first:

- The computer that Cisco Jabber Video for TelePresence is installed on must have IP connectivity to the Cisco VCS. Use ping and traceroute from the PC to verify the IP connectivity.
- If there is a firewall or access control list along the IP route, ensure that it does not block SIP traffic at TCP 5060, UDP 5060, or TLS 5061 in either direction.
- Make sure that the sign-in window shows the correct VCS Control or VCS Expressway address and domain.
- Verify that the login credentials are correct for signing in.

If you could not solve the registration issues by exhausting this list, local logs on the computer can be used to isolate registration issues. If the problem cannot be found, escalate the registration issues to the Cisco VCS administrator.

Poor video quality during a call with Cisco Jabber Video for TelePresence could be caused by several reasons. Most video quality issues can be isolated to the resources available on the computer hosting Jabber Video for TelePresence:

- If multiple applications are open and running at the same time a video call is occurring, the quality of the video being sent and received will be impacted. If this occurs, try closing applications and see whether the quality improves.
- Check the CPU usage during a call. If the CPU usage is close to 100 percent, lower the resolution settings in the Cisco Jabber Video for TelePresence client and call again.
- Using a high-resolution camera that sends video at a rate of 30fps or more can improve video quality as well. Cisco recommends using the Cisco PrecisionHD USB camera.
- On Cisco Jabber Video for TelePresence, you can set the maximum bandwidth limitations in both receive and transmit directions. When setting up a call, the client will not exceed these limits. Jabber Video for TelePresence negotiates the resolution and frames per second to comply with the limits set. The Settings window displays the two sliders that you use to set the bandwidth limits. The minimum bandwidth setting allows Jabber Video for TelePresence to place video calls with a bandwidth rate as low as 24 kbps. The video quality will be very poor if this is attempted, so the minimum recommendation for videoconferencing is at least 384 kbps for reasonable-quality video. Packet loss and jitter that the network causes also affect call quality. Using the i button in the top-right corner of the display will show the packet loss, jitter, and delay suffrages during a call.

Most audio-quality issues are related to the microphone and speakers on the PC hosting Cisco Jabber Video for TelePresence. Using a good-quality headset will resolve these issues. If you experience low or distorted sound when using the Cisco TelePresence PrecisionHD USB Camera Version 1.0 or 1.1 on Windows 7, the issue might be the high input gain that is set for your microphone. This gain can cause sound to be distorted or unnaturally low. Upgrading the camera software to Version 1.5.0 or later, or lowering the recording volume for your microphone in the Windows settings, resolves this issue. If there is no audio output heard during a Cisco Jabber Video for TelePresence call, confirm the following:

- The far end is sending audio, and their microphone is not muted.
- The volume level of your speakers is set to a high enough setting to be heard.
- Your speakers or headphones are not muted.

Be sure to check both the Cisco Jabber Video for TelePresence sound settings and the computer volume control settings, in addition to any hardware switches on your speakers or headphones that can be used to control volume. Confirm that your computer is using the correct sound device. If the far end cannot hear you, check that a microphone is present, connected, and not muted and positioned in an ideal location. For example, if you are using a headset with a pose-able microphone, be sure that it is positioned in front of your chin.

Summary

Understanding how to pull log information and maintain endpoints is critical in any production environment, and becomes an asset in troubleshooting issues when they occur. This chapter focused on how to use the onscreen display, the web interface, and the CLI to collect log information on Cisco TC software-based endpoints. All system information is written to and stored in the Current and Historical log files. This information can be expanded using **debug** commands to offer detailed call traces, which will aid in troubleshooting call setup issues. Administrators should now understand how to perform maintenance on TC software-based endpoints, including how to back up and restore the configuration settings of an endpoint and how to perform an upgrade. Key issues have been identified on TC software-based endpoints that can cause registration, calling, and media issues. These endpoints have tools embedded in them that you can use to troubleshoot these issues.

Cisco CTS software-based endpoints have three logs available that can be accessed through the web interface. These logs continually capture relevant information about the endpoint and can be used to troubleshoot issues when they occur. Because CTS software-based endpoints are controlled entirely by the Cisco Unified CM, troubleshooting steps for these endpoints have been identified in the same manner as troubleshooting other UC or collaboration endpoints within a Cisco Unified CM-centric environment.

Cisco Jabber Video for TelePresence has some tools available locally on the hosting computer that can be use to aid in troubleshooting issues relevant to the soft client. However, because Jabber Video for TelePresence is dependent on the Cisco VCS and the Cisco TMS servers, they are the best tools available for troubleshooting Jabber Video for TelePresence issues. Most issues regarding this soft client will need to be escalated to the VCS or TMS administrator.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 12-4 lists a reference of these key topics and the page numbers on which each is found.

Table 12-4 Key Topics for Chapter 12

Key Topic Element	Description	Page Number
Paragraph	Know the **debug** commands on TC software-based endpoints.	272
Paragraph	Understand current and historical logs on TC software-based endpoints.	274
Paragraph	Know the two backup options on TC software-based endpoints.	275
Paragraph	Understand the process of upgrading TC software-based endpoints.	276
Paragraph	Know the three network test commands that can be used on TC software-based endpoints through the CLI.	278
Table 12-2	Identify the audio/video components that can impact media on TC software-based endpoints.	280
Table 12-3	Identify the different video inputs on a Cisco codec C90.	281
Paragraph	Know the three logs available on CTS software-based endpoints through the web interface.	281
Paragraph	Know the three network test commands that can be used on CTS software-based endpoints through the CLI.	283
Paragraph	Know the Jabber Video for TelePresence minimum and recommended bandwidth rates.	286

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

codec, CoS, DSCP, QoS, SLA, SSH, RTP, SDP, SIP, TLS, URI, MAC

This chapter covers the following topics:

- **Cisco Multipoint Solutions and Product Overview:** This section provides an overview of the Cisco TelePresence MCU and Cisco TelePresence Server products that make up the Cisco multipoint solution.
- **Define Multipoint, Multisite, and Multiway:** This section examines the differences between multipoint calls, the multisite option, and the multiway function.
- **Describe Ad Hoc Multipoint Conferences:** This section examines how the Cisco collaboration edge solution addresses mobile and remote-access issues for businesses.

CHAPTER 13

Cisco Multipoint Solution

Up to this point, the discussions in this book have primarily centered on endpoints. However, even with the plain old telephone system (POTS), the need to conference multiple devices into a single call have been in demand. In video communications, this option is called a multipoint conference. There are different ways of hosting a multipoint conference, whether an endpoint has the ability to host the call or an external multipoint control unit (MCU) is used to host the call.

This chapter discusses the main MCU options available in a Cisco collaboration network. You will learn the definitions of and differences between multipoint, multisite, and multiway. Finally, you will learn about ad hoc calls with use case explanations of when ad hoc calling is used within the Cisco collaboration solution.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 13-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 13-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco Multipoint Solutions and Product Overview	1–7
Define Multipoint, Multisite, and Multiway	8
Describe Ad Hoc Multipoint Conferences	9–10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which multipoint product offers a virtual option for deployment?
   - **a.** Cisco TelePresence MCU
   - **b.** Cisco TelePresence Server
   - **c.** ISR router as a media resource
   - **d.** Cisco TMS
2. Which of the following Cisco TelePresence MCU technology allows endpoints to connect in a conference with different resolutions?
   - **a.** Universal Port technology
   - **b.** ClearVision
   - **c.** Super Resolution Enhancement
   - **d.** Artifact-removal technology
3. Which of the following is a Cisco TelePresence MCU product?
   - **a.** 320
   - **b.** 5320
   - **c.** 7010
   - **d.** 8710
4. Which of the following view modes allows each participant pane to be the same size?
   - **a.** Active speaker
   - **b.** Enhanced continuous presence
   - **c.** Continuous presence
   - **d.** Speaker/participant
5. Which organization manages the TelePresence Interoperability Protocol?
   - **a.** IETF
   - **b.** ITU
   - **c.** IEEE
   - **d.** IMTC

6. Which of the following is not an option for migrating a Cisco TelePresence MCU to a TelePresence Server?

   a. 4510 to 7010
   b. 5320 to 320
   c. 5310 to 310
   d. 8510 to 8710

7. Which of the following features is available on both Cisco TelePresence MCUs and Cisco TelePresence Servers?

   a. Auto-attendants
   b. Cascading
   c. WebEx-enabled TelePresence support
   d. Optimized conferencing

8. What option key must exist on an endpoint to support native multipoint calls?

   a. Multiway
   b. Conference Factory
   c. Multipoint
   d. Multisite

9. What does Cisco define as an ad hoc videoconference call?

   a. Any conference that is not scheduled.
   b. Any endpoint that joins a conference it was not scheduled to join.
   c. Only multiway conferences are considered ad hoc.
   d. All multipoint conference are considered ad hoc.

10. Which of the following options can only support ad hoc videoconferences through a Cisco Unified CM?

    a. Cisco TelePresence MCUs
    b. Cisco TelePresence Servers
    c. Cisco ISR routers with the PVDM2 card
    d. Cisco ISR routers with the PVDM3 card

Foundation Topics

Cisco Multipoint Solutions and Product Overview

Two main media infrastructure platforms are available in a Cisco collaboration solution. The Cisco TelePresence MCU is an industry-leading MCUthat supports either standard-definition (SD) or high-definition (HD) multipoint calls. It delivers high-quality voice and video with an easy-to-use and continuous presence for all conferences. Both H.323 and Session Initiation Protocol (SIP) standards are supported, making it compatible with all major vendor videoconferencing endpoints. Cisco TelePresence MCUs come only in a hardware form and can be deployed as either an appliance server or as a blade server. The Cisco TelePresence Server is a pioneering solution that brings together Cisco TelePresence, HD, and SD videoconferencing users in the same virtual meeting. It preserves the immersive multiscreen experience while connecting to a wide range of endpoints and multivendor telepresence systems and delivers the best call experience for every participant. The Cisco TelePresence Server is available as a hardware appliance or blade, much like the Cisco TelePresence MCU, and is also available as a virtual machine. Table 13-2 illustrates some of the basic differences between these two Cisco multipoint solution options.

Key Topic

Table 13-2 Cisco Multipoint Solution Options

Cisco Multipoint Platform	Call Control Deployment Option	Primary Characteristics
Cisco TelePresence MCU	Cisco Unified CM Cisco VCS	Hardware video bridge for nonimmersive endpoints
Cisco TelePresence Server	Cisco Unified CM Cisco VCS	Hardware or software bridge for immersive and nonimmersive endpoints

The many features that make up the Cisco TelePresence MCU attribute to the superiority it possesses over third-party solutions. All Cisco TelePresence MCU platforms are hardware only and support both SIP and H.323 standards-based multipoint videoconferencing for nonimmersive endpoints. Cisco TelePresence MCUs support video resolutions from SD up to full HD (1080p30 or 720p60). Full HD is available only with an option key. The Cisco TelePresence MCUs also come with voice-only ports so that voice participants do not consume video ports. Cisco TelePresence MCUs support more than 50 different screen layouts, including active speaker and continuous presence view modes. Fully standards compliant, Cisco TelePresence MCUs support video codecs from H.261 to H.264, and audio codecs from G.711 to AAC-LD are supported. This compliancy allows Cisco TelePresence MCUs compatibility with third-party video deployments. The Cisco Video Communication Server (VCS) can escalate calls to the Cisco TelePresence MCU through a feature called *multiway*. Cisco TelePresence MCUs also work with Cisco TelePresence Management Suite (TMS) to support integrated scheduling and device management. With the Web Conferencing option key, the Cisco TelePresence MCUs support a desktop client called ConferenceMe that can be used to join conferences, or unicast and multicast videoconference streaming can be used leveraging Windows Media Player, QuickTime, or Real Time.

Key Topic

Four technologies are incorporated into the Cisco TelePresence MCUs that set them apart from other vendors:

- Universal Port
- Cisco ClearVision
- Cisco Super Resolution Enhancement
- Cisco Artifact Removal

Cisco TelePresence MCUs use a technology known as Universal Port technology. This technology allows each virtual port to be encoded and decoded independently. This ensures that all endpoints connected to a call receive the best quality they are capable of receiving—whether it is HD, ED, or SD. The Cisco TelePresence MCUs are the only multipoint product available that allows HD endpoints in a multipoint call to receive HD resolution while SD and ED endpoints are in the same call. The Cisco TelePresence MCUs are able to transmit HD resolution to HD endpoints by combining the low resolutions into one high-resolution image. Now with ClearVision, the Cisco TelePresence MCUs are able to transmit vastly enhanced SD or ED video to HD endpoints.

Given the extremely large amounts of video processing power available, Cisco ClearVision technology can take SD and ED video and reproduce the image at HD quality with no extra cost in bandwidth. This advanced technology is used in ways never used before in the videoconferencing industry, to vastly improve video quality that SD and ED endpoints can contribute to videoconferences. Cisco ClearVision contains a number of technologies, including the capability to increase the resolution of SD and ED endpoints using Super Resolution Enhancement, and also removes unsightly video artifacts using Cisco Artifact Removal.

With Cisco Super Resolution Enhancement, MCUs can generate higher-resolution images from SD and ED sources, greatly improving the clarity and detail of SD and ED sources in a call. This is carried out automatically and on the fly, using resource-intensive algorithms that enhance the high-frequency visual components, with information gained by analyzing some number of previous video frames and the current frame. In essence, lost, high-frequency, visual elements are replaced with statistically probable alternatives. Cisco Super Resolution Enhancement can produce enhancements of up to four times the source resolutions, and ED resolutions can be enhanced to “near” HD quality.

With Cisco Artifact Removal technology, Cisco provides computationally advanced filters to remove visual artifacts, left by poor endpoints or low-bandwidth encoders (such as 3G devices) to provide improved images. In conjunction with Cisco Super Resolution Enhancement, low-quality and bandwidth-restricted devices will now be able to contribute far better quality video into multipoint calls.

Keep in mind that even with these technologies that improve video quality in place, if there is not enough bandwidth provisioned, or there is no quality of service (QoS) configured during network congestion, user experience will be compromised, resulting in poor video quality. Although QoS and networking go beyond the scope of this class, appropriate considerations still need to be made.

Key Topic

The Cisco TelePresence MCU products are divided into three different classes:

- 4500 series appliances
- 5300 series appliances
- MSE 8000 series

The 4500 series MCUs are all HD only appliance servers except for the 4501. The 4501 is a great entry-level MCU offering 12 SD ports or 6 HD ports or 3 full HD ports. An option key is available that will increase the ports to 24 SD ports, or 12 HD ports or 6 full HD ports. On the high end, the Cisco TelePresence MCU 4520 offers up to 40 high-definition video ports and is an ideal solution for mixed-vendor high-definition endpoint environments. High-definition is defined at 720p30. The limitation of using a 4500 series MCU is the lack of scalability it brings to an environment. If an organization is maxing out the port usage of a 4500 series MCU, they can buy another MCU, but the ports on these two MCUs cannot be joined together without cascading a call. Cascading is when one MCU conference calls into another MCU conference. The full participant layout from one conference will appear in a single pane of the other conference layout. This makes viewing participants very difficult. If cascading is used, best practice suggests using Active Speaker layout.

To offer a lower-cost MCU solution that has some limited scalability available for a customer, Cisco developed the 5300 series MCUs. The Cisco TelePresence MCU 5300 series is the first hardware-stackable MCU appliance in the industry. A serial cable can be used to join up to two 5300 series MCUs together so that they combine their resources and operate as if they were one larger MCU. The Cisco TelePresence MCU 5300 series comes in two models. The 5310 offers up to 20 HD video ports, and the 5320 offers up to 40 HD video ports when they are used in a stack. Some features were removed when Cisco developed these products. The ConferenceMe and streaming option is not available on the 5300 series, nor is the built-in gatekeeper option. However, the 5300 series is still a great option for companies to turn to as they enter the collaboration industry and grow.

The Cisco TelePresence MSE 8000 series is a highly scalable and flexible chassis-based platform for high-definition videoconferencing and voice communication. This powerful, fault-tolerant solution is designed for the mission-critical communication needs of large enterprises. The Cisco TelePresence MSE 8000 series chassis can support up to ten blades and two fan trays. The first slot is reserved for the Cisco Supervisor MSE 8050 blade. The other nine slots can be used for Cisco TelePresence MCU media blades or other Cisco TelePresence MSE 8000 series service blades, in addition to combinations between any of them. The Cisco TelePresence MCU MSE 8510 Media 2 Blade can support up to 80 SD video ports and up to 20 full HD video ports. You can cluster up to three Cisco TelePresence MCU MSE 8510 media 2 blades to support up to 240 SD video participants or 60 full high-definition video participants, plus additional audio-only participants.

It has already been established that the Cisco TelePresence MCU supports over 50 view layouts. What this implies is that every person viewing a conference through an MCU sees a conference layout view. This view divides the video screen into a collection of panes with a different participant video stream displayed in each of those panes. The 50+ layouts available are divided into five different families. These five families can be categorized by three different view modes. Table 13-3 details the different families and layouts for Cisco TelePresence MCUs.

Key Topic

Table 13-3 Cisco TelePresence MCU Layouts, Families and View Modes

Family Description	View Mode
Family 1: Gives prominence to one participant over others	Enhanced Continuous Presence
Family 2: Displays a single participant	Active Speaker
Family 3: Displays the four most active participants without seeing them scaled down to a small size if there are many other participants	Enhanced Continuous Presence
Family 4: Gives equal prominence to up to 20 conference contributors, and is useful for a "role call" of active participants	Continuous Presence
Family 5: Gives prominence to two participants in the center of the view while showing smaller panes of other participants above and below	Enhanced Continuous Presence

With Family 1, the number of contributing conference participants determines the size of the large pane and the number of smaller panes. With Family 2, the participant that is shown is selected via voice switching, when the content channel is being used, or when a participant is assigned the chair (also referred to as being made important). Family 3 is used when there are 5 or more video participants. Only the 4 most active participants will be displayed. With Family 4, the MCU will use a 2x2 layout for up to 4 participants. When a fifth participant joins the conference, the MCU will automatically change the layout to the 3x3 arrangement and will continue to use this layout for up to 9 participants. With 10 or more participants, the 4x4 view is used, and with 17 or more participants the 5x4 view is used. The MCU will continue to use this layout even if there are more than 20 participants. Family 5 works much like family 1, except the 2 most active participants are displayed in the prominent panes. This view is useful for observing a dialog between 2 participants or for viewing slides and a presenter.

Key Topic

The Cisco TelePresence Server supports interoperability between single and multiscreen videoconference systems by using the TelePresence Interoperability Protocol (TIP). TIP is a protocol designed and created by Cisco during the development of the CTS 3000 series Immersive TelePresence room solutions. In Cisco's commitment to interoperability between Cisco TelePresence products and competitive multiscreen video communications devices, Cisco has opened up and transferred TIP to the International Multimedia Telecommunications Consortium (IMTC), making it royalty free for anyone to use. Organizations that want a multistream interoperability option with Cisco can now implement TIP and participate in its ongoing stewardship as a member of IMTC. The TIP specifications describe how to multiplex multiple screens, multiple audio streams, and an auxiliary data screen into a single RTP flow. The TIP specification also defines how Real-time Transport Control Protocol (RTCP) application extensions are used to indicate profile capabilities and per-media flow options as a session is established. In addition, it defines how devices can provide feedback and trigger resiliency mechanisms during the life of the streams.

The Cisco TelePresence Server enables point-to-point and multipoint sessions in addition to a mix of multiscreen and single-screen endpoints. Full high definition supporting 1080p30 and 720p60 is available natively. The Cisco TelePresence Server also supports presentation sharing between SIP endpoints using the Binary Floor Control Protocol (BFCP) and H.323 endpoints using the H.239 standard.

The Cisco TelePresence Server is available as an MSE 8710 blade for the Cisco TelePresence MSE 8000 series chassis. This option is suitable for organizations that already have a Cisco TelePresence MSE 8000, need one to host other blades, or need greater capacity now or in the future. Integrators that want to cluster TelePresence Servers should also use the MSE 8000 chassis. You can include up to 9 blades in each MSE 8000 chassis in addition to the 3550 Supervisory blade. Up to 4 Cisco TelePresence Server MSE 8710 blades can be clustered together to support up to 48 Immersive TelePresence screen licenses using full HD.

The Cisco TelePresence Server is also available as a standalone 7010 server appliance. This appliance server supports up to 12 screen licenses at full HD. The Cisco TelePresence Server 7010 is suitable for organizations with limited rack space and with no existing MSE 8000 implementation. Additional appliance server options are the 300 series TelePresence Servers. Similar to the 5300 series Cisco TelePresence MCUs, the TelePresence Server 300 series are stackable, offering a limited scalable solution. Cisco TelePresence Servers can also be virtualized using VMware ESXi software on the Cisco Unified Computing System (UCS) or third-party specification-based server platforms. Cisco TelePresence Server on Virtual Machine is supported on platforms with either 8 CPUs or 16 CPUs. These deployments have different processing capacities and licensing requirements. All virtual TelePresence Servers support SIP only and are hard-coded to remotely managed mode, meaning they require a Cisco TelePresence Conductor to manage their resources.

Cisco offers the option key to upgrade MCU devices to TelePresence Server for free. Administrators should check to see what resource differences would be caused by a migration to a TelePresence Server. The migration paths are as follows:

- Cisco TelePresence MCU 5310 migrates to the Cisco TelePresence Server 310.
- Cisco TelePresence MCU 5320 migrates to the Cisco TelePresence Server 320.
- Cisco TelePresence MCU MSE 8510 Media 2 Blade migrates to the Cisco TelePresence Server 8710.
- There is no migration path for the Cisco TelePresence MCU 4500 series.

Table 13-4 illustrates the differences between some of the features available on TelePresence Servers and TelePresence MCUs.

Key Topic

Table 13-4 Comparison Chart for TelePresence Servers and TelePresence MCUs

Feature	Virtual TelePresence Server	310/320 TelePresence Server	7010 TelePresence Server	8710 TelePresence Server	4500 MCU	5300 MCU	MSE 8510 Media 2 MCU
Auto-attendant					Yes	Yes	Yes
Cascading					Yes	Yes	Yes
WebEx-enabled TelePresence support			Yes	Yes	Yes	Yes	Yes
Optimized conferencing	Yes	Yes	Yes	Yes			
TIP	Yes	Yes	Yes	Yes			

The layout that the Cisco TelePresence Server chooses for a system depends on the number of connected screens and the characteristics of the other conference participants. A "screen" license on a TelePresence Server refers to the number of codecs (or endpoints) the system uses while in a call. For example, an MX800 has two screens but only one codec, so it would use a single screen license when connected to a TelePresence Server. A Cisco TX9000 has four codes, so it would use four screen licenses. The Cisco TelePresence Server can work with one- to four-screen endpoint systems. It can display any combination of the systems that are participating in a conference to any other type of system in the conference. In general, the behavior of the Cisco TelePresence Server is to display the loudest participants in the most prominent layout panes. If there are more contributors than there are panes available, the quietest participants are not shown.

The Cisco TelePresence Server defaults to segment-switched mode (also called panel-switched) to display participants from Cisco TelePresence rooms. In this mode, the Cisco TelePresence Server independently switches the display of individual cameras from a multiple camera system, based on who is the loudest speaker.

In the room-switched mode, the Cisco TelePresence Server switches the display of all cameras from a multiple camera system, based on who is the loudest speaker. This means that all streams from the cameras of the room are shown on multiscreen endpoints (if they have enough screens). If the loudest speaker is not in the TelePresence room, the Cisco TelePresence Server shows no panels from that room in a large pane.

Cisco active presence (room-switched and OneTable continuous presence) offers a view of all attendees in a meeting while giving prominence to the active speaker. While the active speaker occupies most of the screen, a seamless overlay of others in the call will appear in the lower third of the screen using a "filmstrip" view. This screen layout gives participants a more natural view of everyone sitting around the virtual table. A Cisco TelePresence Server

in OneTable mode contributes three different video streams of the people in the call. As a result, the Cisco TelePresence Server no longer displays the three streams that are received from these systems side-by-side in three adjacent panes but instead displays them on three separate screens.

A single-screen Cisco TelePresence endpoint always receives the panel-switched view when possible, but a participant can change the layout using far-end camera control. In panel-switched view, the loudest participant appears in a full screen with additional participants appearing in up to nine equally sized overlaid panes at the bottom of the screen. The panel-switched view is possible when the other participants in the conference are all single-screen endpoints or a mixture of single-screen endpoints and multiscreen systems that reveal the camera that delivers the loudest audio input. If the panel-switched view is not possible, the Cisco TelePresence Server composes the layout for single-screen endpoints.

Define Multipoint, Multisite, and Multiway

Within a Cisco environment, an understanding of the differences between multipoint, multisite, and multiway needs to be established:

- **Multipoint** is the industry term for a singe conference call that involves three or more participants. This call could be hosted by an MCU or by an endpoint.
- **Multisite** is the option key on Cisco endpoints that enables that endpoint to host multipoint calls.
- **Multiway** is simply call forwarding or call escalation. When two endpoints are in a point-to-point call, a third endpoint can be dialed. After the third call connects, the multiway-capable endpoint can select a "join" or "merge call" option, and all three endpoints will be transferred to an MCU, which will host the multipoint call. To use multiway, one of the endpoints must support the multiway feature. All endpoints involved must support call hold and call transfer. There must be a Cisco MCU, and a VCS must be involved with appropriate settings configured.

Cisco TelePresence multisite is the simplest form of multipoint conferencing that is available. One video endpoint can host three to four participants in a call using its embedded multipoint capability. As each endpoint connects to the host, the video and audio streams are composited into a single transmission that is sent out to all the participants. Consider a scenario where endpoint A and endpoint B are connected in a point-to-point conversation. During this conversation endpoint A can call endpoint C, or answer an inbound call from endpoint C, without the call between endpoint A and B ever being interrupted. The call is automatically made a multipoint call using the Multisite option key on endpoint A as endpoint C is connected to the call.

This form of multipoint conferencing is effective for small conferences, but it does have some limitations. *Scaling* is an issue because the host endpoint must mix the audio and video from every other endpoint. Therefore, the size of the conference in most cases is limited to four or five participants, of which one endpoint is a multisite host. There are additional *bandwidth* requirements for endpoints with embedded multisite capabilities. *Endpoint consistency* is another potential limitation. Not all endpoints have multisite capabilities. The *user experience* can be impacted, depending on the multisite endpoint model.

There are limitations in video resolution and the number of participants that can join a call hosted using multisite. This limitation can degrade the overall user experience when compared to calls that are hosted on a dedicated MCU. The view modes are also limited as compared to dedicated MCUs.

Cisco centralized multipoint devices, such as the Cisco TelePresence MCU or Cisco TelePresence Server, offer more features and scalability with conferencing such as transcoding, trans rating, and so on. Cisco TelePresence multiway uses centralized MCU resources. Cisco TelePresence endpoints that do not have embedded multisite capability can use multiway to initiate multipoint conferences on an MCU.

With Cisco TelePresence multiway, making conference calls is intuitive. If you make a call to a new party, having put your first party on hold, you are offered the choice to join all parties into a Cisco TelePresence multiway conference. This procedure also applies if you receive a call when you are already on a call and choose to accept it. Without escalating the call, you can also switch between each party to continue any point-to-point conversations you are having. To make multiway operational, you need to configure the Cisco VCS, an MCU, and endpoints that support the multiway option. Figure 13-1 illustrates a call scenario that leverages the multiway feature.

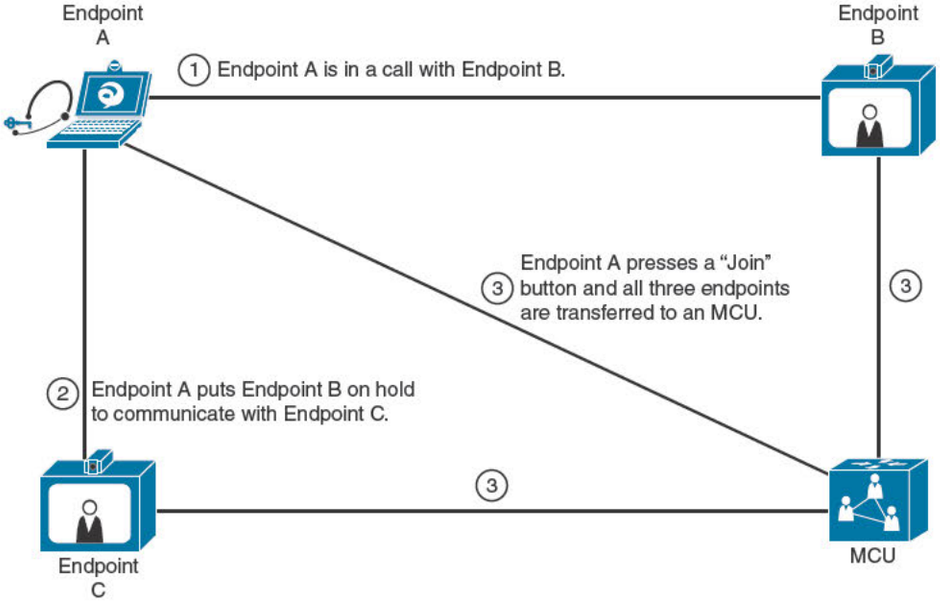


Figure 13-1 *Multiway Function in a Cisco Collaboration Environment*

In Figure 13-1, video endpoint A calls video endpoint B. All call setup signaling is routed through the Cisco VCS, but the media is point to point. After the call is established, endpoint A initializes a second call endpoint C, which will automatically place endpoint B on hold. Once this call leg is established, endpoint A and C are in a point-to-point call, while B is still on hold. By pressing the *join* or *merge call* buttons, endpoint A will initialize a third

call leg by sending the endpoint-configured multiway URI to the Cisco VCS. This multiway URI will match the multiway URI configured in the Cisco VCS Conference Factory setting, which communicates to the VCS that the endpoint is trying to escalate all connected parties to an MCU for a multipoint call. The Cisco VCS forwards a conference URI to a designated Cisco TelePresence MCU device. The Cisco VCS then connects A, B, and C with the Cisco TelePresence MCU using several H.323 or SIP call-signaling messages. Endpoints A, B, and C are connected to the Cisco TelePresence MCU in a multipoint conference using the multiway call-escalation feature.

All Cisco TelePresence TC software-based endpoints support Cisco multiway. Other Cisco or third-party endpoints can be invited to Cisco TelePresence multiway conferences using SIP and H.323 standards-based signaling. These other endpoints must support call hold and call transfer. H.323 uses a *Route to MC* facility message for call transfer, and SIP uses the *SIP Refer* message. Other call infrastructure elements, such as ISDN video gateways, must also support the messages when they are in the call path.

Describe Ad Hoc Multipoint Conferences

The definition of ad hoc is "on the fly." Therefore, multipoint ad hoc conferencing is defined as any multipoint conference that is not scheduled. More specifically in a Cisco environment, an ad hoc call is referred to any endpoint that is not scheduled for a call. There are different types of ad hoc conferences that are based on different deployments and ad hoc use scenarios. A point-to-point call between two endpoints could be considered an ad hoc call. A multipoint call using the Cisco TelePresence multisite option could be considered an ad hoc call as well. Both of these call scenarios could be scheduled through TMS, but without TMS, they will always be considered ad hoc. The Cisco multiway feature is always considered to be an ad hoc call. By its very nature, multiway can never be scheduled.

Within a Cisco Unified CM environment, both ad hoc and rendezvous conferencing are supported. The ad hoc feature within a Cisco Unified CM environment works similarly to the multiway feature of a VCS. When a point-to-point call is initiated, the call setup signaling is routed through the Cisco Unified CM, but the media flows between the two endpoints. When one of the participants selects the *conference* button on a phone, the second participant is placed on hold, and a third-party can be dialed. Once the second call leg is established, the *conference* button can be selected again, which signals the Cisco Unified CM that an ad hoc conference is requested. The Cisco Unified CM will select an appropriate media resource and transfer all the participants to the MCU.

The rendezvous feature can be very elaborate and warrants a deeper discussion that goes beyond the scope of this book. Rendezvous conferences pertain to ad hoc calling, however, and involve a dialing out to preconfigured endpoints after the first endpoint has joined the rendezvous conference. Another dial-out scenario uses the Cisco TelePresence MCU graphical user interface (GUI) user tools to dial out to endpoints manually from the MCU. Other participants may connect to a conference by dialing the conference ID directly from their endpoint.

When a participants want to meet with other participants, an MCU conference can be dialed. The endpoint connects to the MCU services based on the dialed address. Direct

service numbers and service number ranges are configurable on MCUs, called conference IDs. To directly connect to a preconfigured conference, the endpoint dials a provided conference ID. The statically preconfigured permanent conferences are directly reachable by dialing the configured numbers or URIs. To browse through preconfigured conferences, the endpoint dials into the MCU through an auto-attendant, which is commonly reachable through a number range or a service prefix.

Key Topic

Cisco UC endpoints support ad hoc conferencing using simple buttons to escalate point-to-point conversations to a multipoint conference. This function is also supported for video using the Cisco TelePresence MCU that the Cisco Unified CM controls as a video multipoint resource. The Integrated Services Routers (ISR) can support audio ad hoc multipoint conferences with the PVDM2 card, and with the Cisco High-Density PVDM3 card, the Cisco ISR can be used for ad hoc videoconferences. The protocol between the Cisco Unified Communications Manager and the Cisco TelePresence MCU that is used for media resource control is HTTP. The ISR and Cisco Unified Communications Manager use Skinny Client Control Protocol (SCCP) for media resource control. Cisco Unified Communications endpoints, such as Cisco Unified IP videophones and Cisco Jabber, support ad hoc videoconference initialization through the native Cisco Unified Communications conferencing features. The Cisco Unified CM also has built-in audio conference bridging capability for a limited number of participants.

Summary

Multipoint communication has been defined in this chapter as any communication involving three or more participants. Many options are available within a Cisco collaboration network that accommodates multipoint communication. The Cisco TelePresence MCUs have appliance and blade servers that support nonimmersive multipoint calls. The 5300 series MCUs offer limited scalability, and the MSE 8510 Media 2 Blade MCU offers a higher level of scalability. Four unique technologies are incorporated into these products that make them superior to third-party products on the market. The Cisco TelePresence Servers offer multipoint communications between immersive and nonimmersive endpoints. These server platforms come in appliance and blade form, in addition to a virtual server that can be built on your own ESXi server. The Cisco TelePresence 5300 series MCUs and the 8510 Media 2 blades can be upgraded to a TelePresence Server.

There are different types of ad hoc calls in a Cisco collaboration environment. The multisite option key on endpoints allows them to host multipoint calls natively. Without TMS, these multisite calls are considered ad hoc. A point-to-point call can be escalated to a multipoint ad hoc call hosted on an MCU using the multiway feature on a TC software-based endpoint. Ad hoc calls are also defined as an endpoint that manually dials into an MCU conference or auto-attendant. If an administrator manually dials out from an MCU to an endpoint, this would also be considered an ad hoc call.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 13-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 13-5 Key Topics for Chapter 13

Key Topic Element	Description	Page Number
Table 13-2	Hardware and software options for MCUs and TelePresence Servers	294
Paragraph	Four technologies incorporated into Cisco TelePresence MCUs	295
Paragraph	Three classes of Cisco TelePresence MCUs	296
Table 13-3	View modes and layout families	297
Paragraph	TIP protocol	297
Paragraph	Migration paths from Cisco TelePresence MCUs to TelePresence Servers	298
Table 13-4	Feature comparison between Cisco TelePresence MCUs and TelePresence Servers	299
Paragraph	Multipoint, multisite, and multiway	300
Paragraph	Ad hoc conference	302
Paragraph	ISR router with PVDM2 and PVDM3 cards	303

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

POTS, MCU, multipoint, multisite, multiway, ad hoc, SD, HD, Full HD, TMS, ConferenceMe, Universal Port technology, ClearVision, Super Resolution Enhancement, Artifact Removal technology, TIP

This page intentionally left blank

This chapter covers the following topics:

- **Cisco TelePresence MCU Installation:** This section provides an overview of the necessary steps to install an appliance MCU.
- **Cisco TelePresence MCU Basic Setup for Cisco VCS Registration:** This section examines the configuration settings needed for an MCU to register to the Cisco VCS.
- **Cisco TelePresence MCU Basic Setup for Cisco Unified CM Registration:** This section examines the configuration settings needed for an MCU to register to the Cisco Unified CM.
- **Cisco TelePresence MCU Conference Creation and Management:** This section explains how to create conferences on the Cisco MCU, and examines the tools available to manage conferences.
- **Cisco TelePresence MCU Troubleshooting:** This section examines the logs available on an MCU that can be used to troubleshoot problems.

Cisco TelePresence MCUs

The TelePresence multipoint control unit (MCU) products that Cisco uses today were originally developed by a company call Codian. TANDBERG acquired Codian in 2007, and Cisco acquired TANDBERG in 2010. Cisco TelePresence MCUs have several advanced technologies embedded that make them a superior product from their inception through today.

This chapter focuses on how to install a Cisco TelePresence appliance MCU. You will also understand the basic settings that need to be configured to register an MCU to the Cisco Video Communications Server (VCS) and to the Cisco Unified Communications Manager (CM). This chapter also delves into the different logs available on the MCU that you can use to troubleshoot issues as they develop.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 14-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 14-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco TelePresence MCU Installation	1–2
Cisco TelePresence MCU Basic setup for Cisco VCS Registration	3–5
Cisco TelePresence MCU Basic Setup for Cisco Unified CM Registration	6
Cisco TelePresence MCU Conference Creation and Management	7–8
Cisco TelePresence MCU Troubleshooting	9–10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What CLI command enables you to configure an IP address on the MCU?

   a. **xcommand**
   b. **xconfiguration**
   c. **configuration**
   d. **static**

2. What CLI command enables you to reboot the MCU?

   a. **shutdown**
   b. **reboot**
   c. **xcommand reboot**
   d. **xcommand boot**

3. What protocols can be used with MCU registration?

   a. H.323 only on the Cisco Unified CM
   b. H.323 and SIP on the Cisco VCS
   c. H.323 and SIP on the Cisco Unified CM
   d. H.323 and SIP on the Cisco Unified CM and the Cisco VCS

4. What setting can be configured on an MCU that prepends a prefix on conference IDs when registering them to the Cisco VCS?

   a. MCU Service Prefix
   b. Prefix for MCU Registration
   c. Incoming calls to unknown conferences and auto attendants
   d. Media Port Reservation

5. What setting can be configured on an MCU that registers to the VCS and forwards all calls to the MCU regardless of the digits dialed after it?

   a. MCU Service Prefix
   b. Prefix for MCU Registration
   c. Incoming calls to unknown conferences and auto attendants
   d. Media Port Reservation

6. When registering an MCU to the Cisco Unified CM, what setting must be configured after the media resource group?

   a. Regions
   b. Add to a Device
   c. Media Resource
   d. Media Resource Group List

7. Which of the following is an option when creating an ad hoc conference on the MCU?

   a. Conference ID
   b. Auto attendant
   c. PINs
   d. Conference name

8. Which of the following is an option when managing conferences from the MCU?

   a. Extending the conference
   b. Transferring a participant to another MCU
   c. Texting
   d. Creating breakout sessions within the conference

9. Which of the following can be observed using the Statistics menu of a participant from within the MCU?

   a. Packet loss
   b. Capability sets
   c. Latency
   d. Bearer channels

10. Which of the following logs allows administrators to view who last logged in to the MCU?

    a. Event log
    b. SIP/H.323 log
    c. Audit log
    d. CDR log

Foundation Topics

Cisco TelePresence MCU Installation

How Cisco TelePresence MCUs are initially installed is slightly different depending on if an administrator is installing an appliance MCU or a blade server. Any device that communicates across a network must have basic network settings configured before packets can be sent out. Cisco TelePresence blade MCU network settings are configured through the Supervisory blade of the MSE 8000 blade chassis. This section focuses on how to configure an appliance Cisco TelePresence MCU network settings.

On the front of the panel of the appliance MCU, there is a Console port. The cable needed to connect to this console port is an RS232-to-RJ-45 serial cable. Connect the RJ-45 connector of the cable to the Console interface of the MCU. Connect the RS232 connector on the cable to a PC. An RS232-to-USB converter may be needed if your computer does not have a serial port built-in. Open a terminal session like PuTTY. Change the connection type to Serial. Set the Serial line to the Com port to which the cable is connected on the PC, and configure the remaining settings as follows:

- **Speed (baud):** 38400
- **Data bits:** 8
- **Stop bits:** 1
- **Parity:** none
- **Flow Control:** none

Once the terminal session has been configured, start the session. On the Cisco TelePresence MCU, connect the network cable to the LAN port on the front panel. Connect the power cable to the MCU, and the unit should begin the power-up process. This can be observed from the terminal session.

The Cisco TelePresence MCU uses Dynamic Host Configuration Protocol (DHCP) by default. Best practice suggests that the IP settings should be changed to a static IP address. Once the MCU has completed the boot process, you can issue a simple command from the terminal session to change these parameters. In the terminal session, enter the command **static** *ip-ddress subnet-mask default-gateway dns-address*, and press the **Enter** key. Even though your organization may not use Domain Name System (DNS), something must still be entered into that field. You can either enter a public DNS address or use the default gateway address again. After the static IP address settings have been configured, the MCU needs to be rebooted to bind the network settings to the server. Type the command **shutdown**. The system will go through a shutdown process, but only the services will be stopped. When the interface receives the message "The MCU has shut down," enter the command **boot**. This initiates a process where the MCU will shut down the rest of the

way and reboot, this time using the new static IP address assigned to it. When the Cisco TelePresence MCU has finished the reboot process, the administrator can web into the unit through a web browser.

To finalize the initial setup of the Cisco TelePresence MCU, a few settings need to be verified, and possibly changed, through the web interface. Open a web browser and navigate to the IP address of the MCU. Log in with the username **admin** and leave the Password field blank. Figure 14-1 shows the menus that are available once an administrator logs in to the MCU.

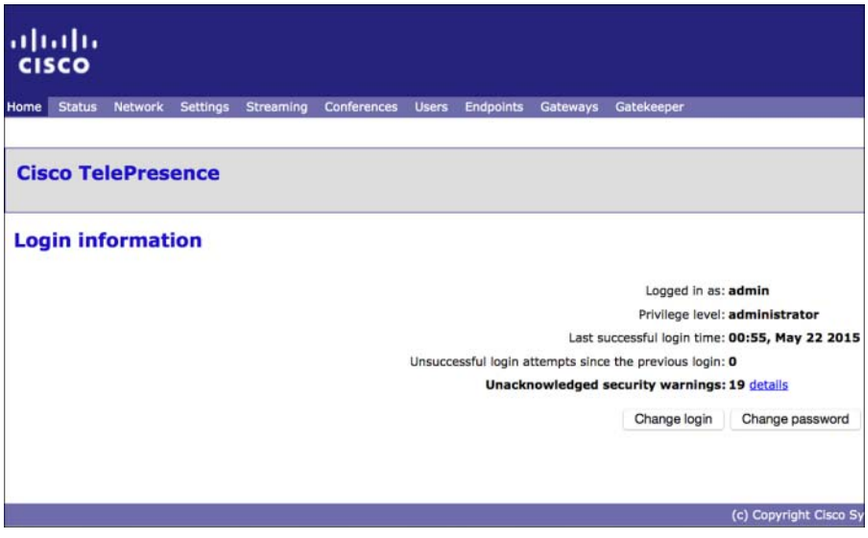


Figure 14-1 *Cisco TelePresence MCU Main Menus*

Select the **Network** menu, and under the Port A submenu, scroll down to the **Port A IP Status** section. Verify that the correct IP address information is displayed. Scroll down farther to the Port A Ethernet Status section and verify that the **Duplex** is negotiated at **Full Duplex**. If the Duplex is negotiated at Half Duplex, this setting will need to be changed on the MCU and on the router from **Automatic** to **Full Duplex**. Changing this setting in both places will prevent duplex mismatch from occurring. Figure 14-2 identifies the network settings available through the web interface.

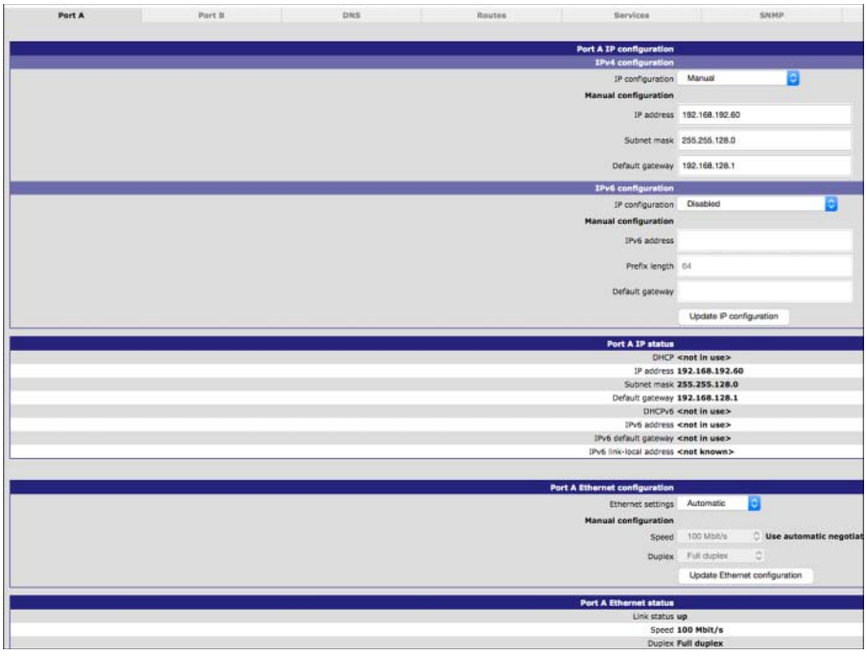


Figure 14-2 *Cisco TelePresence MCU Network Settings*

Next, click the **DNS** menu and enter the hostname and domain for the MCU. Together these two settings make up the DNS A record as it would appear within the DNS server. A secondary DNS address can be entered at this time as well. The hostname is also the system name. This will appear in TMS after the MCU is added. Click the **Update DNS Configuration** button. Verify that the information is displayed correctly under the DNS Status section. Figure 14-3 identifies the DNS settings available through the web interface.

Click the **Services** menu. Ensure that all the services you intend to use are enabled by checking the box beside the port number, and ensure that the port numbers match the ports used within your network. Default port numbers are displayed automatically. The TCP services available on the MCU include HTTP, HTTPS, Incoming H.323, SIP (TCP), Encrypted SIP (TLS), Streaming (Windows Media Player), Streaming (other), FTP, and ConferenceMe. Streaming and ConferenceMe are not available in the Cisco TelePresence MCU 5300 series. The UDP services available on the MCU include SNMP, SIP (UDP), H.323 gatekeeper, and tunneled media. Simple Network Management Protocol (SNMP) is used by the TelePresence Management Suite (TMS) to manage the Cisco TelePresence MCU. SIP (UDP) and H.323 gatekeeper are used for registration to the Cisco Video Communications Server (VCS). Figure 14-4 identifies the Services menu settings available through the web interface.

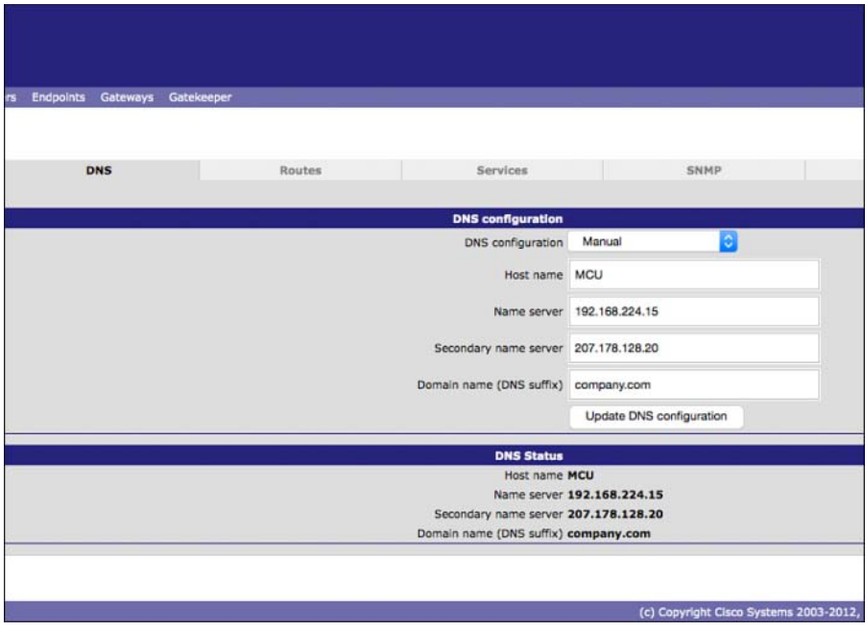


Figure 14-3 *Cisco TelePresence MCU DNS Settings*

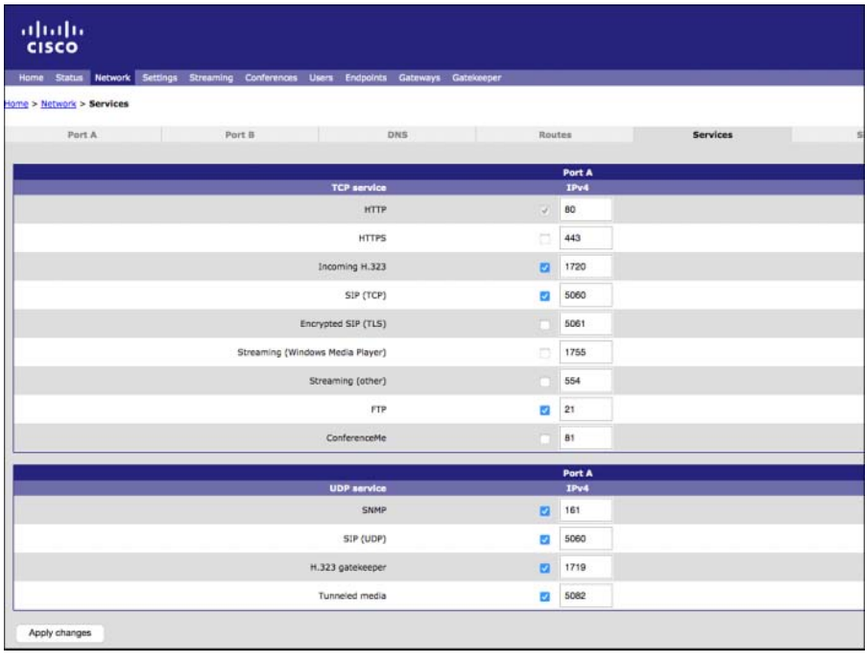


Figure 14-4 *Cisco TelePresence MCU Service Settings*

Because the admin account does not use a password by default, a password must be created to secure the MCU. Click the **Users** menu on the main menus across the top of the page. Click the blue **admin** account hyperlink. This will take you into the configuration page. Under the Change Password section, leave the **Current Password** box blank, and enter a password in the **New Password** and **Re-Enter Password** sections. Click the **Update Password** button. This changes the password for the MCU. A confirmation box may appear asking for confirmation as to which account the password was changed. Click the admin account and click **OK**. The initial setup of the Cisco TelePresence MCU is now complete. Figure 14-5 identifies the settings used to change the admin password through the web interface.

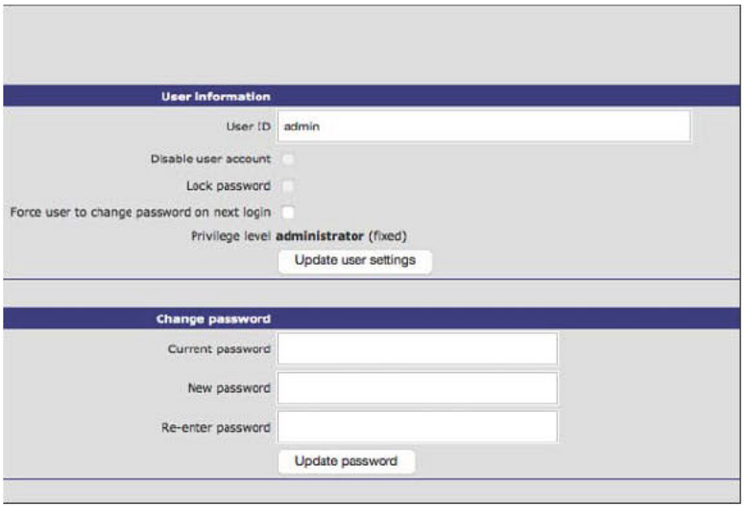


Figure 14-5 *Changing the Cisco TelePresence MCU Admin Password*

Cisco TelePresence MCU Basic Setup for Cisco VCS Registration

Key Topic

Once the network settings have been configured and validated, the Cisco TelePresence MCU can be configured for registration. The settings that need to be configured for registration will vary depending on whether the MCU registers to the Cisco VCS or the Cisco Unified Communications Manager (CM). The MCU can register to the Cisco VCS using H.323 or Session Initiation Protocol (SIP).

On 4500 series MCUs and the MSE 8510 Media 2 blades, there is a menu called Gatekeeper. This menu option is a remnant of the days before TANDBERG bought Codian. Codian did not have a call control device, so they built a gatekeeper into their MCUs and ISDN gateways. This built-in gatekeeper only allowed for H.323 registrations for the purpose of mapping aliases to IP addresses, which made calling easier. There were no other security or call control functions of this gatekeeper. After TANDBERG bought Codian, they limited the number of registrations to the built-in gatekeeper to 25 registrations, which made it a great startup solution for small businesses. If customers wanted to scale their solution to support additional registrations, the VCS was the next-step solution offered. After Cisco bought

TANDBERG, they developed another MCU based on the Codian product called the 5300 series, removing the built-in gatekeeper along with some other functions, such as the streaming feature. If you want to register the Cisco TelePresence MCU to the Cisco VCS using H.323, do not use the Gatekeeper menu. This feature is disabled by default. Enabling this feature and registering the MCU to the Cisco VCS will cause routing issues.

To register the Cisco TelePresence MCU to the Cisco VCS requires the administrator to click the **Settings** menu. Under the Settings menu, click the submenu called **H.323**. Under this menu, configure the following settings:

1. H.323 gatekeeper usage: **Enabled**.
2. H.323 gatekeeper address: *IP address of the VCS*.
3. Gatekeeper registration type: There are several choices under the gatekeeper registration type. Using the information button in the top right corner, indicated by an **i**, will open another page with descriptions to aid in finding out which type to use.
4. Ethernet port association: Select the port (A or B) and IP type (IPv4 or IPv6) you are using.
5. H.323 ID to register: Enter the H.323 ID for the MCU. Dialing this H.323 ID from an endpoint will call into the Default Auto Attendant.
6. In the Prefix for MCU Registrations and MCU Service Prefix fields, enter the prefixes for the MCU.

Figure 14-6 shows the H.323 settings on the Cisco TelePresence MCU.

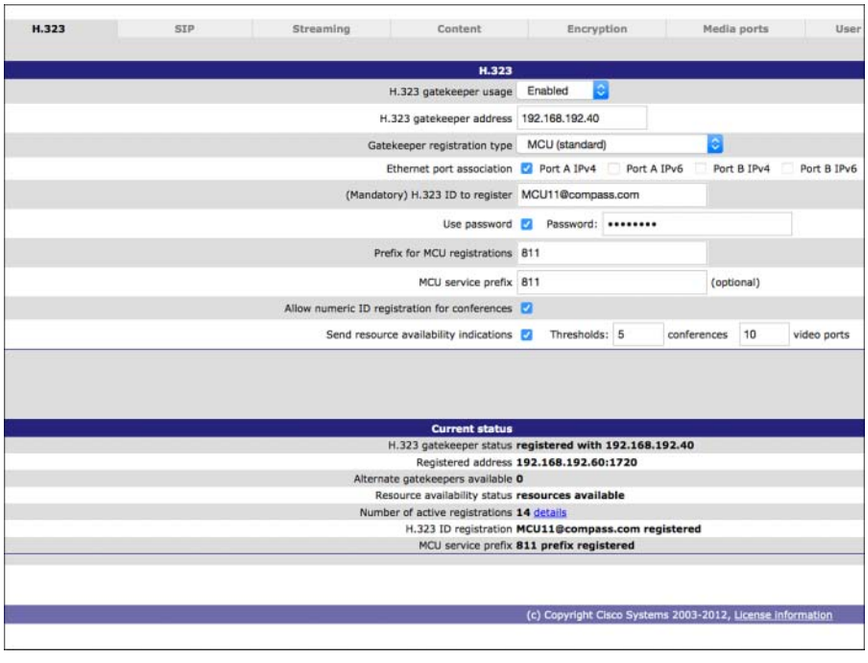


Figure 14-6 *H.323 Settings on the Cisco TelePresence MCU*

To explain the differences between these two prefix options, consider this scenario. Assume there are four endpoints registered with different H.323 E.164 aliases to the Cisco VCS in the following order: 5001, 5002, 5003, and 5004. A conference is also created on the MCU that is trying to register with the conference ID of 5004, following the same dial plan used with the endpoints. A problem is introduced because the endpoint with the alias 5004 conflicts with the conference ID of 5004. On the VCS, the registration conflict mode will not allow duplicate H.323 aliases to register to the VCS. If this setting is configured with reject mode, the conference 5004 will never register with the VCS because it will conflict with the endpoint 5004. Therefore, when endpoint 5001 dials 5004, the VCS will always connect the call with the endpoint 5004, even if the endpoint 5001 wants to connect with a conference on the MCU. Figure 14-7 illustrates this scenario.

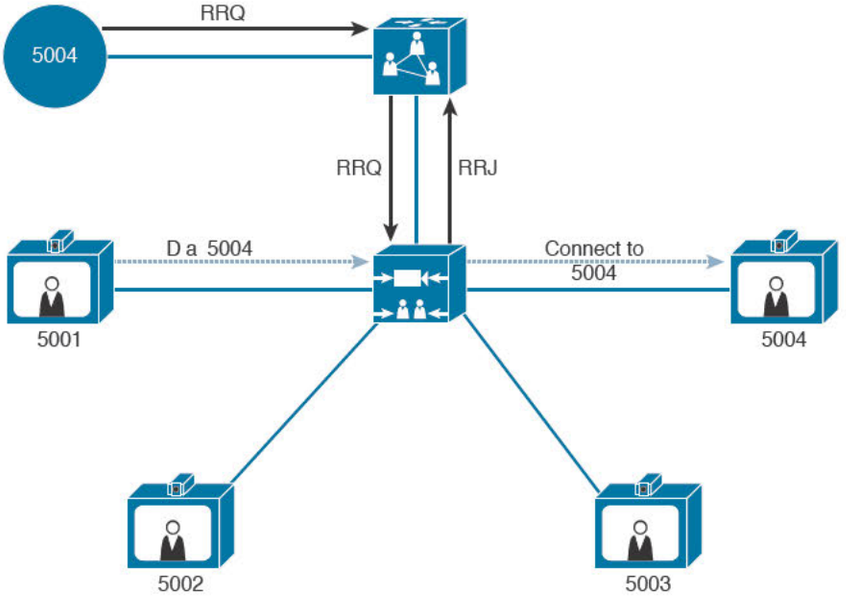


Figure 14-7 *Alias Conflicts Between MCU Conference IDs and Endpoint E.164 Aliases*

Key Topic

The solution is to create a prefix for MCU registration. The prefix for MCU registration differentiates between aliases assigned to endpoints from aliases assigned to conferences. Once a prefix for MCU registration is created, any conference created on the MCU that is configured to register to the VCS will be prepended with this prefix. To resolve this scenario, the MCU is configured with a prefix for MCU registration of 8. Therefore, when conference 5004 is created, it will register to the VCS as 85004. Now when endpoint 5001 decides to dial 85004, the VCS knows to connect the call with the MCU, which in turn strips the prefix and connects the call to conference 5004.

Key Topic

Another problem can be introduced using the same setup as the preceding scenario. Assume endpoint 5004 dials 85008, which is not a conference currently scheduled on the MCU. Because the VCS is not aware of this conference, it will respond with an ARJ (admission reject). Whether the caller is trying to create an ad hoc conference or simply misdialed

the conference ID, there is a way to ensure that the caller still has options rather than just being disconnected from the call attempt. To resolve this issue, you need to configure the MCU service prefix. The MCU service prefix will register to the VCS. Any alias dialed that begins with this prefix is routed to the MCU regardless of the remaining digits. Because all calls beginning with that prefix are routed to the MCU, the MCU must be configured with how to deal with these calls when they come through. To configure this setting, click the **Conferences** tab, scroll toward the bottom of the page to the **Incoming Calls to Unknown Conferences and Auto Attendants** setting, and select the desired parameter. Figure 14-8 illustrates the Incoming Call to Unknown Conferences And Auto Attendants menu options.

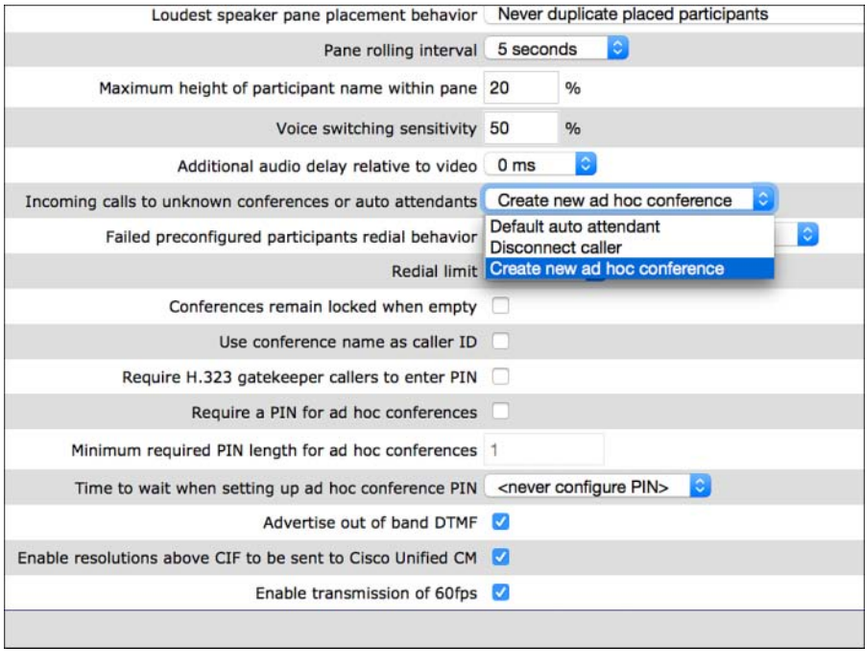


Figure 14-8 *Incoming Call to Unknown Conferences and Auto Attendants Menu Options*

The options are as follows:

- **Default Auto Attendant:** Will route calls to the default auto attendant.
- **Disconnect Caller:** Will drop the call. Normal call clearing will be displayed as the reason the call was dropped in the VCS.
- **Create an Ad Hoc Conference:** The MCU will create a new conference using the alias dialed as the conference ID.

After the MCU service prefix has been configured and registered to the Cisco VCS, when endpoint 5004 dials 85008, the VCS will only look at the 8, strip the prefix, and route the call to the MCU. The MCU will then perform the task configured in the Incoming Calls to Unknown Alias or Auto Attendants setting. In this scenario, the MCU creates an ad hoc conference with a conference ID of 5008. Figure 14-9 illustrates how this process works.

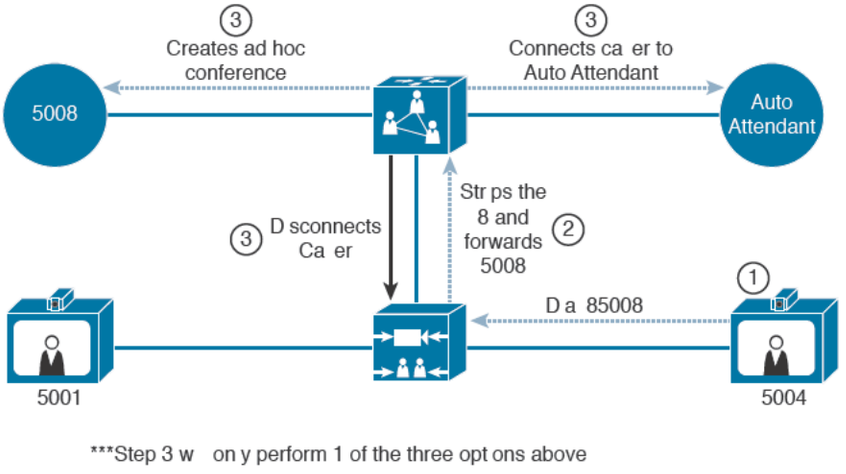


Figure 14-9 *Call Routing Using the MCU Service Prefix*

Both the MCU service prefix and the prefix for MCU registration can be configured with the same digits. The last configuration setting that must be configured for H.323 registration is the **Allow Numeric ID Registration for Conferences** setting. If the desired behavior is for conferences created to register to the VCS, this box must be checked. After all the H.323 registration settings have been configured, click the **Apply Changes** button to save the settings. In the Current Status window below the configuration menus, you can verify the registration status.

While under the Settings menu, select the **SIP** submenu to configure SIP registration on the Cisco TelePresence MCU to the Cisco VCS. Ensure the **SIP Registrar Usage** setting is configured to **Enable**. Only the domain used for SIP should be configured in the **SIP Registrar Domain** field, not the full URI for the MCU. The hostname of the URI must be configured separately under the **Username** field. The Username field should not be the full URI either. The reason these settings are separated is because when conference IDs, which are only in numeric value, register with the VCS as SIP, the MCU will append the domain configured in the SIP Registrar Domain field to the end of the conference ID to form a URI for the SIP registration. The username is the hostname for the SIP URI of the MCU. Dialing this full URI will call the default auto attendant. If the desired behavior is for conferences created to register to the VCS, the **Allow Numeric ID Registration for Conferences** box must be checked. Under the SIP Call Settings section, enter the IP address or URL of the VCS to which you want the MCU to register. After clicking the **Apply Settings** button, you can confirm registration on the right side of the SIP registrar usage section at the top of the page. Figure 14-10 shows the SIP settings on the Cisco TelePresence MCU.

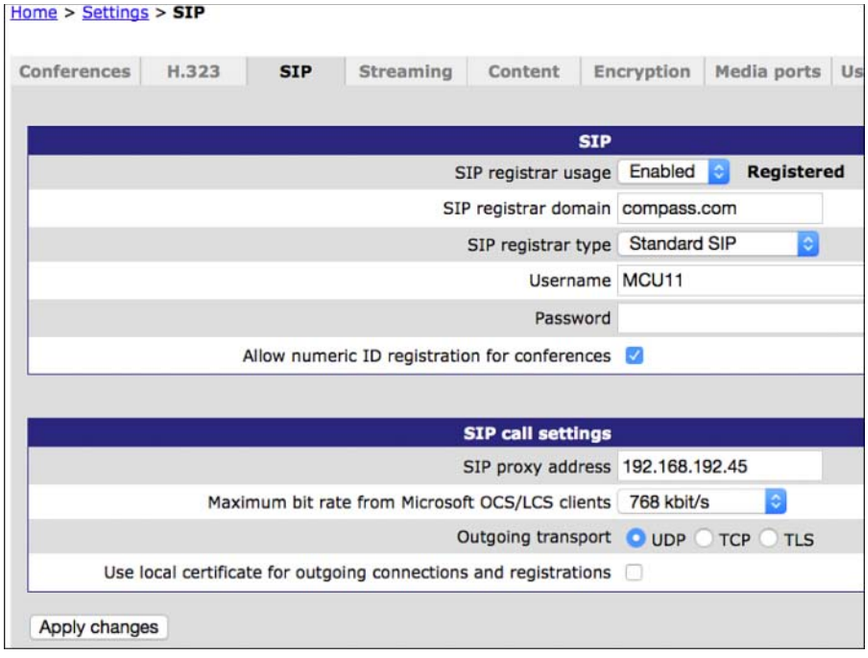


Figure 14-10 *SIP Settings on the Cisco TelePresence MCU*

Cisco TelePresence MCU Basic Setup for Cisco Unified CM Registration

In a deployment in which the Cisco TelePresence MCU is registered to the Cisco Unified CM, the MCU acts as a media resource for the Cisco Unified CM. Media resources are services that allow the Cisco Unified CM to perform functions, like transcoding and music-on-hold. In this case, the service the Cisco Unified CM offers is multipoint conferencing. Deploying an MCU with the Cisco Unified CM only allows no support for scheduling. Instead, the MCU can be used for ad hoc or rendezvous conferences. It is important to note, however, that the Cisco TelePresence MCU can only be used as either an ad hoc conference resource or a rendezvous conference resource. A single MCU cannot fulfill both functions. This section discusses how to configure the Cisco TelePresence MCU as an ad hoc bridge. If the Cisco TelePresence MCU is deployed as a rendezvous conference bridge, and TMS is used to manage the MCU, conferences can be scheduled through TMS.

To register the Cisco TelePresence MCU to the Cisco Unified CM, you need to configure the following settings. **Media Port Reservation** needs to be set to **Disabled**. When enabled on the MCU, this setting requires scheduled conferences to specify the number of ports needed. This ensures ports are available at the time conferences are scheduled to launch. If media port reservation is enabled in a typical deployment, the native ad hoc function on the MCU is disabled. Also, extending conferences on the MCU will not be allowed. This setting

can be configured on an MCU by navigating to **Settings > Conferences**. Once the Media Port Reservation setting has been configured, scroll down to an advanced setting called Incoming Calls to Unknown Conferences or Auto Attendants mentioned in the previous section. The Cisco Unified CM needs the ability to create ad hoc conferences on the Cisco TelePresence MCU. Unlike in a Cisco VCS-centric environment, the Cisco TelePresence MCU does not need to be pointed to the Cisco Unified CM to register. Ensure that H.323 and SIP are disabled on the Cisco TelePresence MCU.

The means in which a Cisco Unified CM leverages media resources is through a function call media resource group lists. Media resource group lists provide a list of media resource groups the Cisco Unified CM can choose from, depending on the function needed at hand. Media resource groups are a grouping of media resources made available to the Cisco Unified CM. Therefore, for the Cisco Unified CM to use the Cisco TelePresence MCU as a media resource for multipoint conferencing, it needs to be added to the Unified CM as a conference bridge. Figure 14-11 illustrates a flow chart for the media resource process on the Cisco Unified CM.

Key Topic

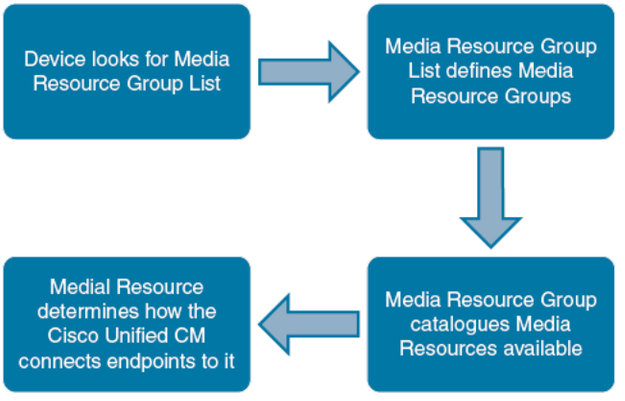


Figure 14-11 *Flow Chart for the Media Resource Process on the Cisco Unified CM*

Configuring the elements of the flow process in Figure 14-10 needs to be in reverse order. Beginning with the media resource on the Cisco Unified CM, navigate to **Media Resources > Conference Bridge**. Click the **Add New** button. Under Conference Bridge Type, select **Cisco TelePresence MCU** for the conference bridge type. Under the HTTP Interface Info section, check the **Override SIP Trunk Destination as HTTP Address** box, fill out the appropriate fields, and click **Save** when finished. The MCU has now been added to the Cisco Unified CM, and the status should show as Registered. Figure 14-12 shows the settings that need configured to add an MCU as a media resource on the Cisco Unified CM.

Before the added MCU can be used as a media resource, it needs to be added to a media resource group. Add the MCU to a media resource group by navigating to **Media Resources > Media Resource Group**. Click **Add New**, create a name for the group, click the media resource created in the previous step, and move the MCUs into the Selected Media Resources area. Click **Save** when finished. Figure 14-13 illustrates how to add media resources to a media resource group (MRG).

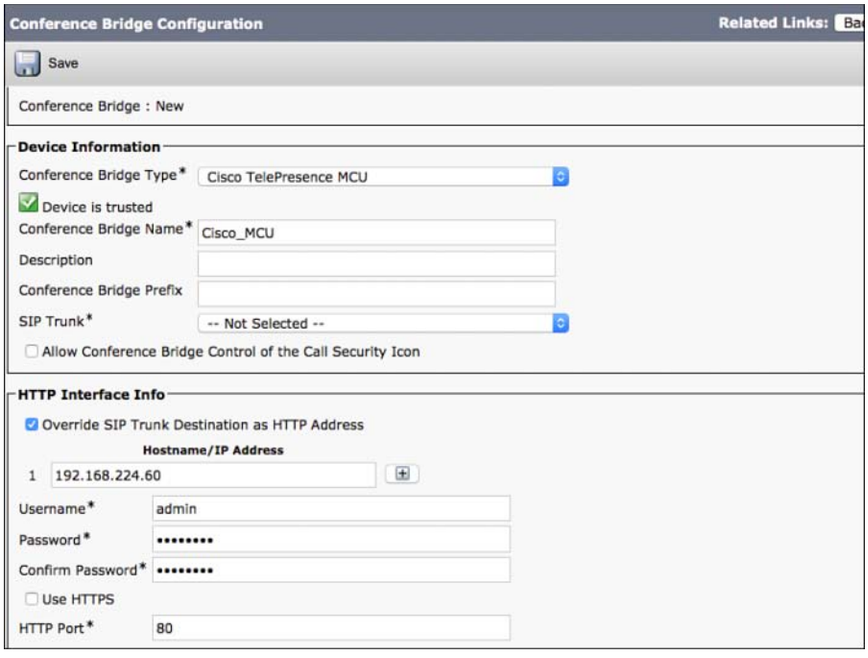


Figure 14-12 *Adding a Media Resource on the Cisco Unified CM*

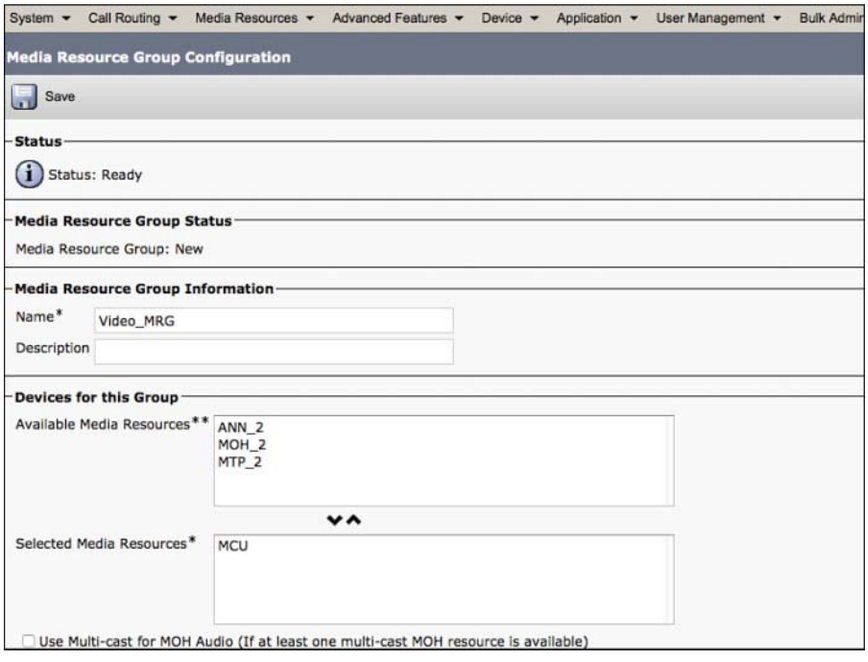


Figure 14-13 *Adding Media Resources to an MRG*

The media resource group now needs to be placed within the appropriate media resource group list. Go to **Media Resources > Media Resource Group List** and click **Add New**. Create a name and move the previously created media resource group into the Selected Media Resource Groups area, and then Click **Save**. Media resources in the MRG, and MRGs in the media resource group list, will be used based on the order they are listed. Administrators should be very careful what order is used. Also, Cisco Unified CM is used for both voice and video communications, and each may use different resources. Therefore, best practice is to create a separate MRG and media resource group list (MRGL) for voice and video resources. Figure 14-14 illustrates how to configure an MRGL.

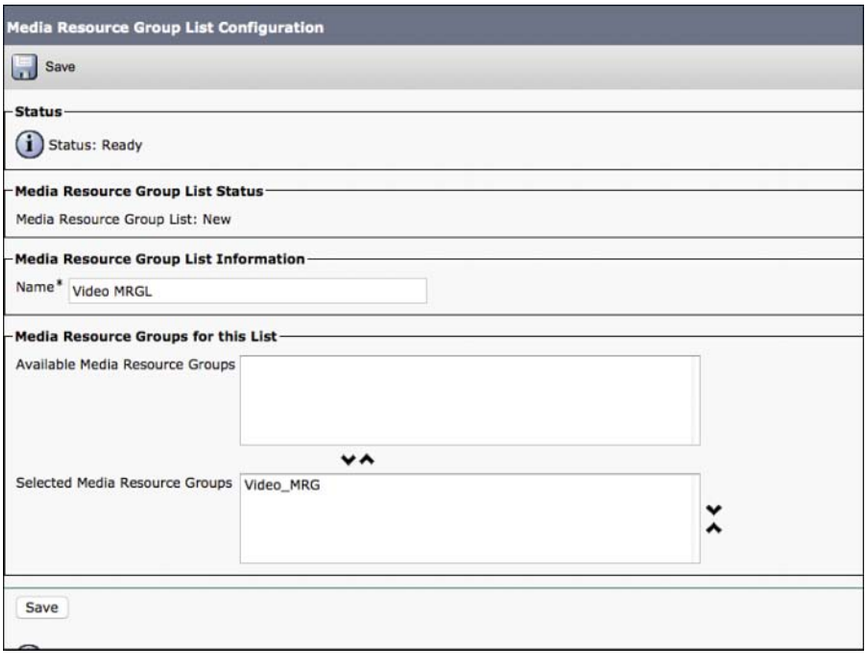


Figure 14-14 *Adding MRG to MRGL*

The media resource group list now needs to be attached to a device to be able to make use of the MCU for ad hoc conferencing. Go to **Device > Phone** and select a device. Choose the MRGL that you created earlier. Click **Save** and **Apply Configuration** when finished. Rather than adding the MRGL to every endpoint on the Cisco Unified CM, it can be added to a device pool instead. Every endpoint that is part of that device pool will automatically use the MCU as the media resource for ad hoc conferences. To add the MRGL to a device pool, go to **System > Device Pool**. Click an existing device pool, or click **New** to create a new one. Scroll down under the Roaming Sensitive Settings section and select the appropriate MRGL from the Media Resource Group List menu. Because some devices may already be using this device pool, select **Save** and **Apply Configuration** when finished. Figure 14-15 illustrates how to add an MRGL to a device pool.

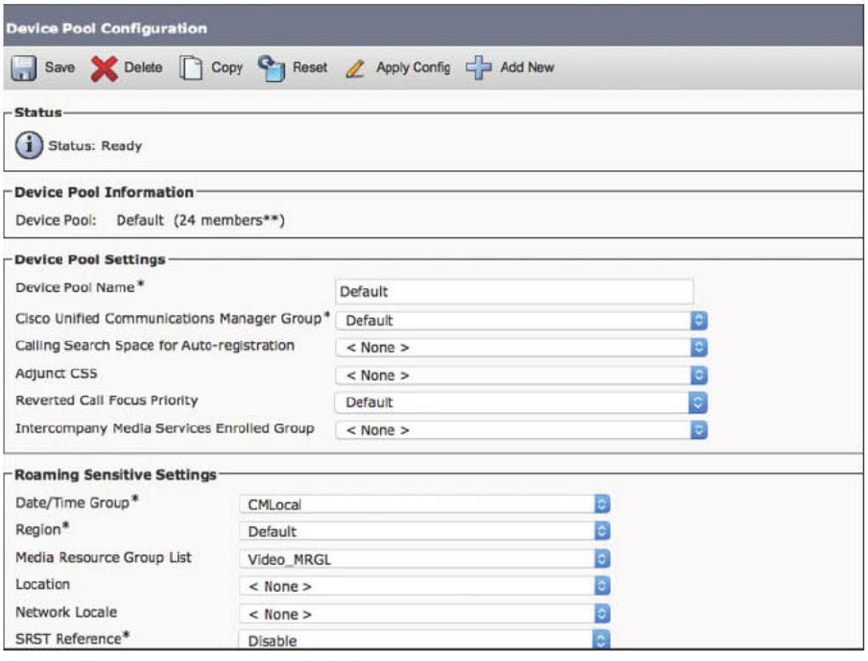


Figure 14-15 *Adding an MRGL to a Device Pool*

Cisco TelePresence MCU Conference Creation and Management

The Cisco TelePresence MCU has embedded auto-attendant features. Interactive visual and interactive voice response (commonly termed IVR) features are supported. The Cisco TelePresence MCU also has a default auto attendant preconfigured. Customized auto-attendant setups are possible either by modifying the default auto attendant or by creating a new one. When you dial into a conference, you can connect directly to your conference or into the auto-attendant menu, which presents you with a series of options. From the auto attendant, you can select the conference that you want to join or create an ad hoc conference, as long as this option is enabled.

Key Topic

You can create an ad hoc Cisco TelePresence MCU conference using the auto attendant as follows:

Step 1. Dial the Cisco TelePresence MCU auto-attendant alias to get the MCU IVR.

Press the star key (*) to create a new conference.

Step 2. Enter the number of the conference that you want to create, followed by the pound key (#).

Step 3. Entering the PIN is an option that is enabled under the global conference settings. The use of a PIN can be enabled as an option or a requirement. If a PIN is enabled as an option and you are prompted to create a PIN but do not want to create one, waiting for a set duration of time will take you into the conference without PIN protection. If a PIN is required, the creator of the conference cannot start it without creating a PIN first. When prompted, create the PIN and press **#**. You will then be connected to the conference.

Other participants can dial directly into the created conference using the conference ID used to create the ad hoc conference.

An alternative to ad hoc conferences can be scheduled in advance. On the web interface of the Cisco TelePresence MCU, click the **Conferences** menu. Four submenus will be displayed. Under the Conference List submenu, there are three sections: Active Conferences, Scheduled Conferences, and Completed Conferences. Figure 14-16 illustrates how this menu will appear.

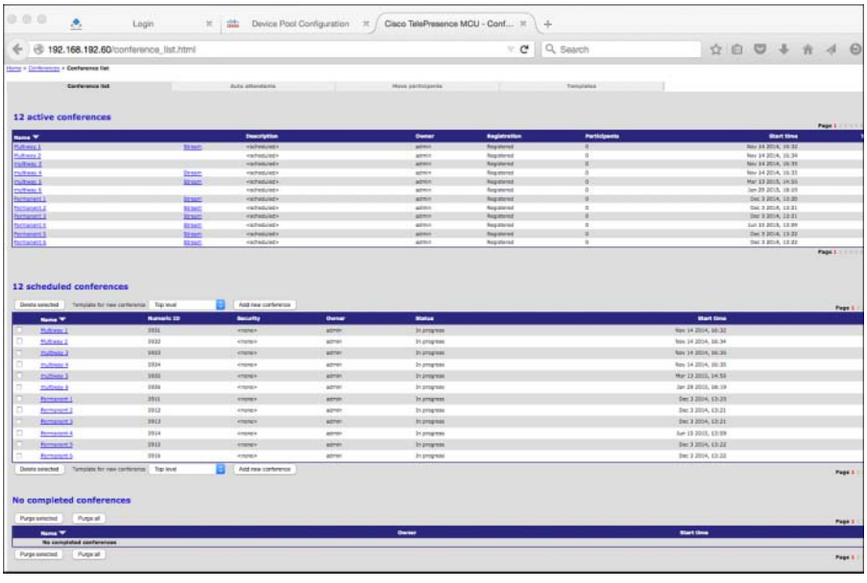


Figure 14-16 *Conference Menu on Cisco TelePresence MCU*

Beside the Scheduled Conferences section, click the **Add New Conference** button. The only configuration field that is required is the Name field. Enter a name for your conference. If you want participants to be able to dial directly into the conference, a numeric ID must also be configured. This scheduled conference can be protected with a PIN as well.

Scrolling down will allow the administrator to configure the start date, start time, and duration of the conference. It can be made persistent so that once it is started the conference will never expire. Reoccurring settings can also be configured. If none of these parameters are configured and the conference is saved as is, the conference will start immediately and last for 1 hour by default. Click the **Add Conference** button located on the right of the screen either at the top of the page or at the bottom. Now participants can access this conference by either dialing the conference ID or via the auto attendant. Figure 14-17 illustrates some of the menus available under the MCU Conference Creation section.

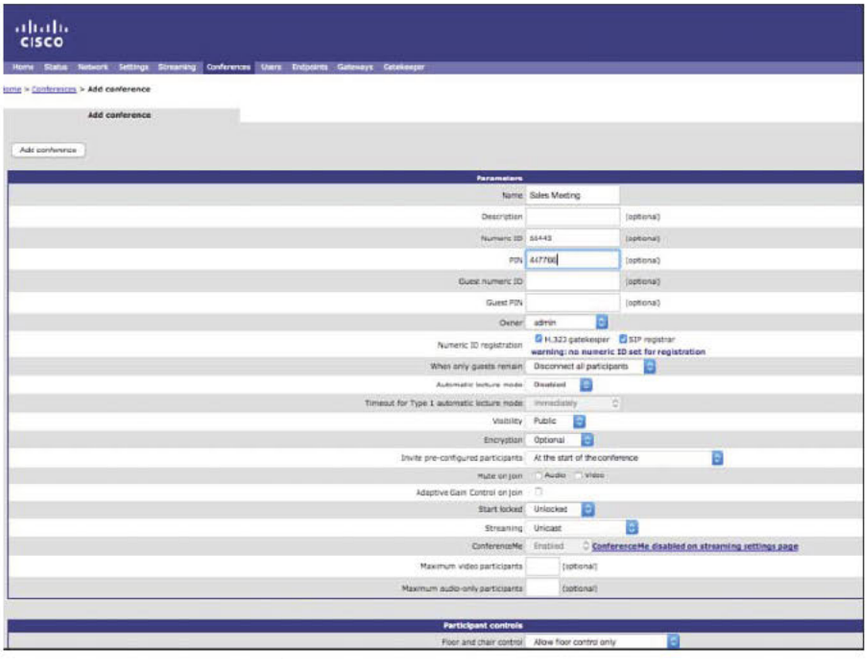


Figure 14-17 *MCU Conference Creation Section*

Key Topic

Conferences that are hosted by a Cisco TelePresence MCU can be monitored through the MCU web interface. Under the same Conferences menu and Conference List submenu where scheduled conferences are created, click the blue hyperlink of a conference under the Active Conferences section. Figure 14-18 shows the management page that will be displayed once a conference is selected.

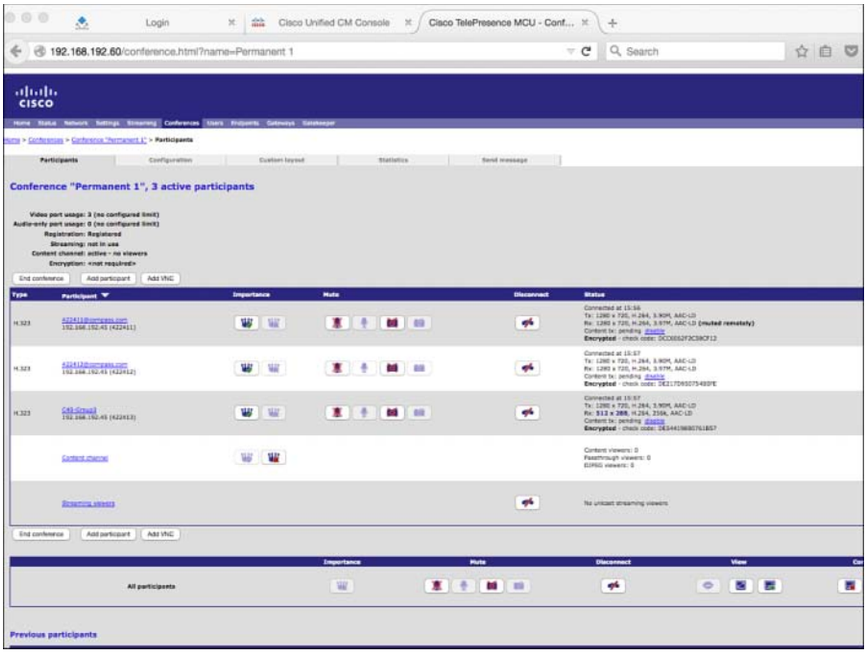


Figure 14-18 *Cisco TelePresence MCU Conference Management*

As shown in Figure 14-18, the conference details page can be used to verify the connected call status parameters. The relevant headings above the Participants section are used to verify status details: the type of the call; participant name or alias; and status, which details the connection time, transmit and receive codecs, resolutions, and bandwidth rates. The headings marked Importance and Mute allow administrators to assign chair control, mute the audio, and mute the video of each participant. The submenu tabs at the top of the page allow conference administrators to change settings like the layout all participants will use, and a text message can be sent to all participants in the conference, which will be displayed on their monitors. If an administrator were to click the blue hyperlink of a participant under the Participant heading, a new list of submenus would be accessible. From here, conference administrators can customize settings for that particular participant, send private text messages to their endpoint, and even view statistic and diagnostic settings specific to their connection with the MCU. The next section focuses more on what information can be obtained using the Statistics and Diagnostics tabs for participants. Figure 14-19 illustrates the submenu tabs available when a specific endpoint is selected.

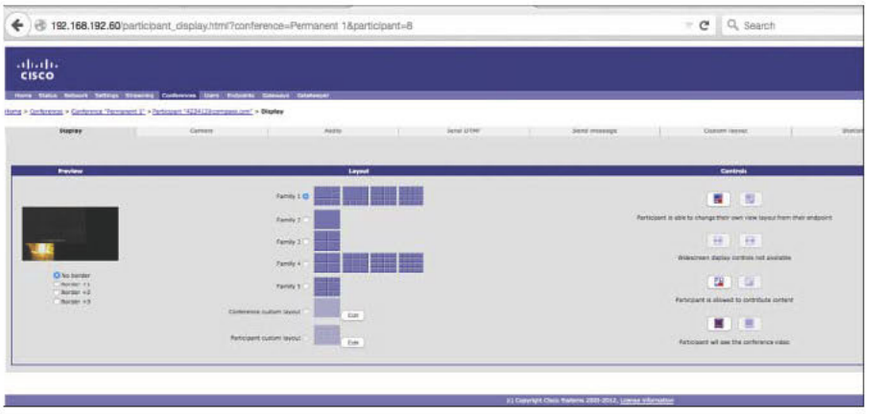


Figure 14-19 *Endpoint Submenus on a Cisco TelePresence MCU*

Cisco TelePresence MCU Troubleshooting

Several tools are available on the Cisco TelePresence MCU that you can use to troubleshoot issues. As mentioned previously, statistics and diagnostics information is available on each participant connected to a conference. There are also event logs, H.323/SIP syslogs, audit logs, and call detail record (CDR) logs. Administrators can also download diagnostic information and conference information. A health page can be used to view the health of hardware components, and there is a tool that can be used to test connectivity between the Cisco TelePresence MCU and other devices.

To view the statistics and diagnostics information of an endpoint's connection with the MCU, go into the management tool of a conference and select an endpoint connected to that conference. Click the **Statistics** tab. This information is very useful when trying to find out why the Cisco TelePresence System is experiencing issues with quality. From the audio statistics, you can see the actual codec that is used as well as jitter and packet errors for audio streams. In addition to audio statistics, you can see video statistics. You can see the actual bandwidth that is used and jitter and packet errors for video streams. Table 14-2 outlines the information displayed using this Statistics menu tool.

Key Topic

Table 14-2 MCU Participant Statistics Information

Audio Media Statistics	Video Media Statistics	Content Media Statistics	Control
Received	**Received**	**Received**	**Received**
Receive Stream	Receive Stream	Receive Stream	RTCP Receive Address
Receive Address	Receive Address	Receive Address	Receiver Reports
Encryption	Encryption	Encryption	Packet Loss Reported
Received Jitter	Channel Bit Rate	Channel Bit Rate	Sender Reports
Received Energy	Received Bit Rate	Received Bit Rate	Other

Audio Media Statistics	Video Media Statistics	Content Media Statistics	Control
Packets Received	Received Jitter	Received Jitter	
Packet Errors	Delay Applied for Lipsync	Packets Received	
Frame Errors	Packets Received	Packet Errors	
	Packet Errors	Frame Rate	
	Frame Rate	Frame Errors	
	Frame Errors		
Transmit	**Transmit**	**Transmit**	**Transmit**
Transmit Stream	Transmit Stream	Transmit Stream	RTCP Transmit Address
Transmit Address	Transmit Address	Transmit Address	Packets Sent
Encryption	Encryption	Encryption	
Packets Sent	Channel Bit Rate	Channel Bit Rate	
	Transmit bit Rate	Transmit bit Rate	
	Packets Sent	Packets Sent	
	Frame Rate	Frame Rate	
	Temporal / Spatial	Temporal / Spatial	

Using the Statistics tool, an administrator can see the actual bandwidth that is used and jitter, packet errors, and the codec that is being used. Clicking the **Diagnostics** tab will display capabilities exchanged between the endpoint and the MCU. At the top of the page is a Status section with general call information like send and receive bandwidth rates. Below that is the Endpoint-Supplied Information section that displays the system name, E.164 alias (when applicable), product, and version. The third section is Media Capabilities. This section lists all the audio, video, and other codecs that were sent to the endpoints and received from the endpoint. Figure 14-20 shows what information is found on the Diagnostics tab of a connected endpoint on the MCU.

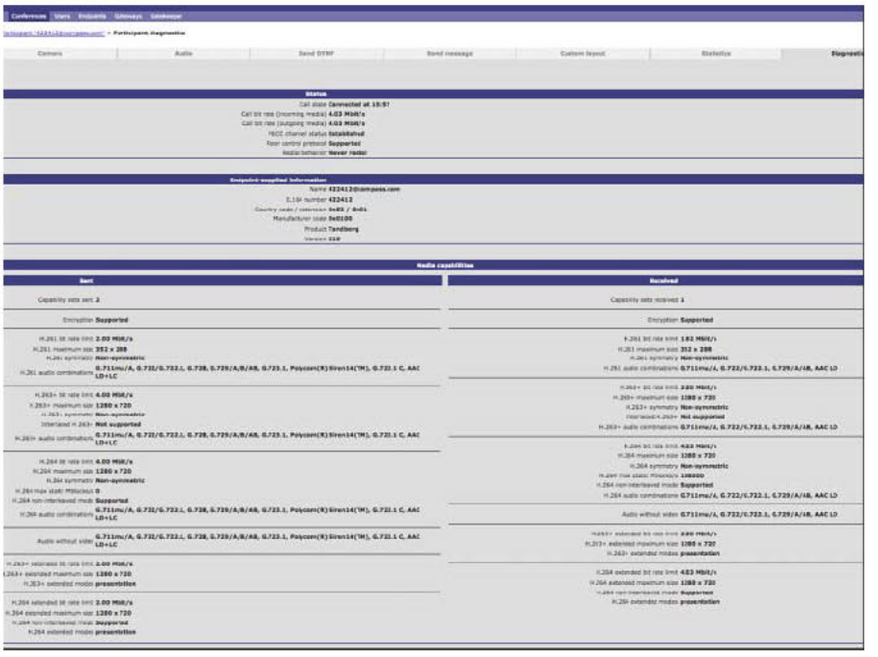


Figure 14-20 *Cisco TelePresence MCU Endpoint Diagnostics Page*

Key Topic

Logs can be accessed on the MCU by clicking the **Logs** menu in the top-right corner of the screen. This is the only main menu option not listed with the other main menus. Several logs are available, each with its own unique function. The Event log provides basic event status for MCU operations. The events available in the Event log include info, warning, and error. The event capture filter can be used to change the level of information available in the Event log. The H.323/SIP log allows administrators to take detailed call traces. This should not be enabled except at the time an issue needs to be traced to find the root cause. The information is stored locally on the MCU. Because this log contains a high level of information, it can fill up very quickly. If the log were to fill up, it would affect the performance of the MCU. This information can be stored on a remote server using the **Syslog** tab. The event display filter controls the level of trace the H.323/SIP log provides. The Audit log is used to log user information. Every user who logs in to the Cisco TelePresence MCU will be recorded within this log. It displays the username, when the user logged in, what the user changed, and when the user logged out, with time stamps on every entry. This information is not detailed, so the Audit log can be enabled and left on. The CDR log is a call detail record that shows all participant interaction with conferences and auto attendants on the MCU. All of these logs can be downloaded in Extensible Markup Language (XML) format and can be manually deleted if they become too full. Figure 14-21 shows the different log tabs available on the Cisco TelePresence MCU.

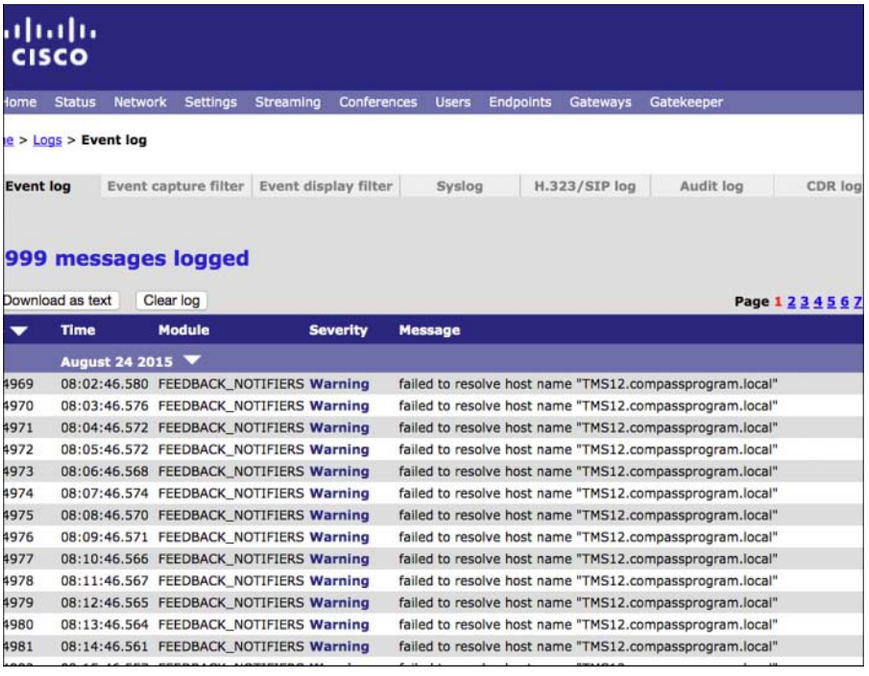


Figure 14-21 *Logs Tabs on the Cisco TelePresence MCU*

Under Status in the main menus, the General submenu allows administrators to download diagnostic and conference information. This is generic information representing the whole MCU. Figure 14-22 shows the menu options available here.

Also under the Status menu is the Health submenu. This section will display the health of system hardware components, including fans, voltage, temperature, and the RTC battery. Status is shown as Current Status and Worst Status Seen. The standing can be OK or Out of Spec. If the standing is Out of Spec under Worst Status Seen but OK under Current Status, click the **Clear** button and monitor the MCU to see whether the problem repeats itself. If the standing says Out of Spec under Current Status, you need to take immediate action to resolve the issue. Figure 14-23 shows the Health menu options on the MCU.

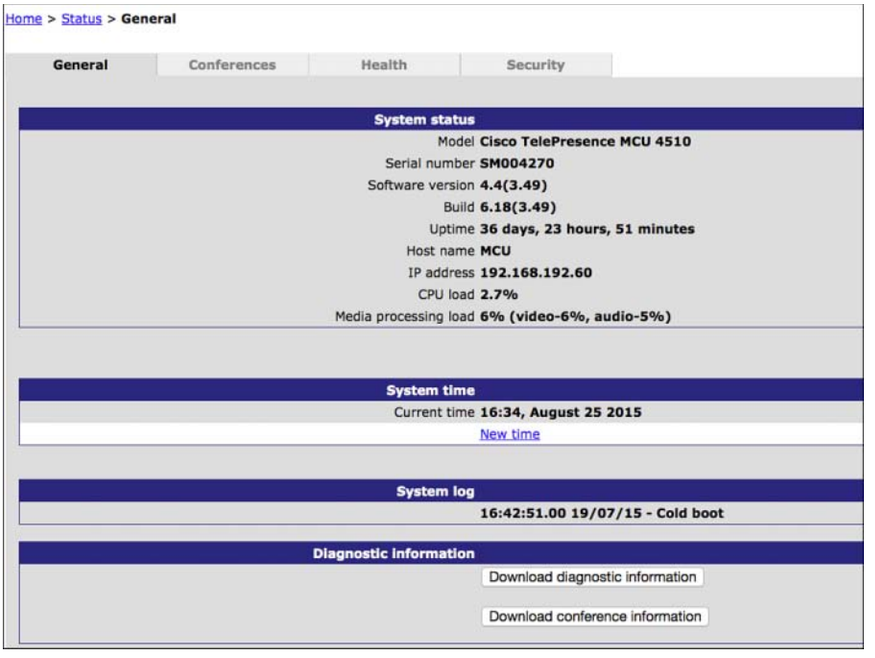


Figure 14-22 *Status Menu Options on the Cisco TelePresence MCU*

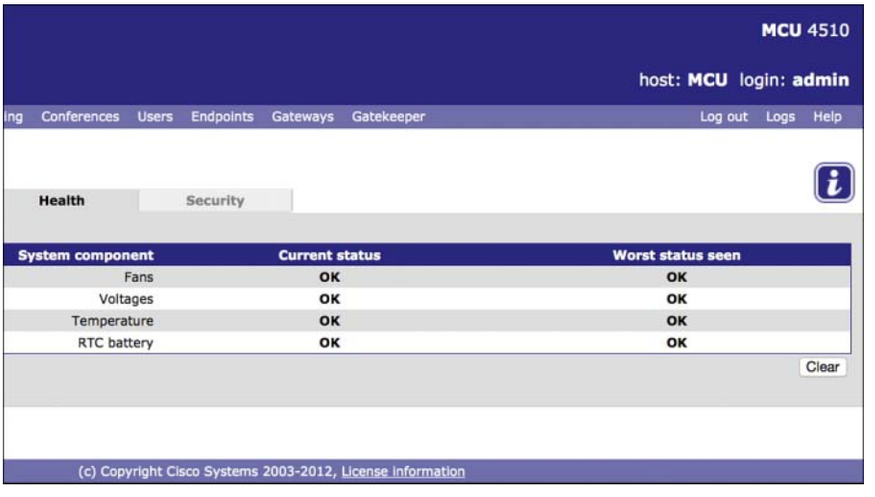


Figure 14-23 *Heath Menu on Cisco TelePresence MCU*

If an endpoint is unable to call into a conference, it could be a network-related issue preventing connectivity between that endpoint and the MCU. A tool on the MCU enables administrators to test the connectivity to any other device within the network. Click the **Network** main menu and the **Connectivity** submenu to access this tool. In the box beside Remote Host, enter the IP address of the device you are testing connectivity to, and then click the **Test Connectivity** button. The MCU will run a **ping-route** to that device and display the information in the window to the right. Figure 14-24 illustrates the use of the network connectivity test tool on the Cisco TelePresence MCU.

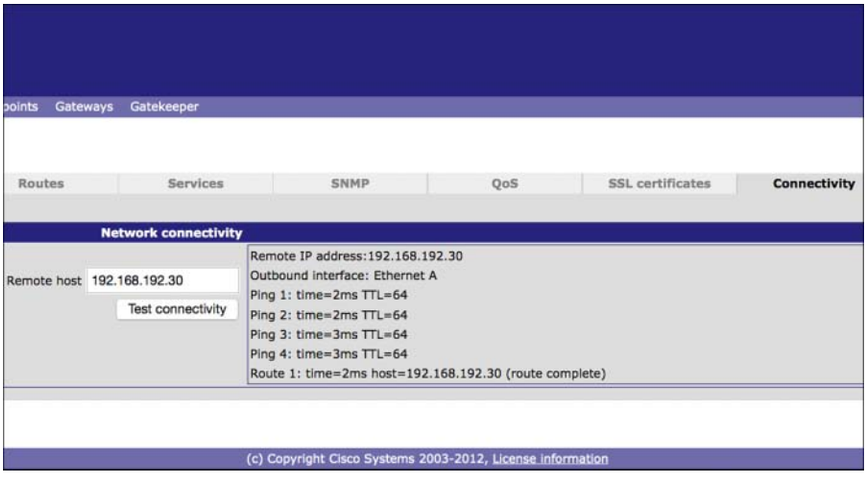


Figure 14-24 *Cisco TelePresence MCU Network Connectivity Tool*

Summary

After completing this chapter, you should understand how the Cisco TelePresence MCU is configured, operates, and the native tools available on the MCU for troubleshooting used within your environment.

This chapter examined how to install a Cisco TelePresence appliance MCU. After an MCU is installed, configuration settings need to be set up to register to the Cisco VCS, which supports both H.323 and SIP registration from the MCU. A unique set of configuration settings need to be configured on the MCU for registration to the Cisco Unified CM. The MCU does not actually point or reach out to the Cisco Unified CM for registration. Adding the MCU as a media resource on the Cisco Unified CM will establish registration. This chapter also covered how to create and configure both ad hoc and scheduled conferences and how to manage conferences after they have started. This chapter also assessed different logs and tools available on the MCU that you can use to troubleshoot issues as they develop.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 14-3 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 14-3 Key Topics for Chapter 14

Key Topic Element	Description	Page Number
Paragraph	Statically assign IP addressing using a serial connection	310
Paragraph	Processes for MCU registration	314
Definition	Prefix for MCU registration.	316
Definition	MCU service prefix.	316
Figure 14-11	Ad hoc calls flow process	320
Paragraph	Ad hoc calls through the MCU auto attendant	323
Paragraph	Management options on the MCU	325
Table 14-2	Statistics tab for endpoints on the MCU	327
Paragraph	Logs on the MCU	329

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

MCU service prefix, prefix for MCU registration, conference, ad hoc, media resource, media resource group, media resource group list, CDR, auto attendant

This chapter covers the following topics:

- **Cisco TelePresence Server Installation:** This section examines the steps required to install an appliance TelePresence Server.
- **Cisco TelePresence Server Basic Setup for Cisco VCS Registration:** This section examines the configuration settings needed for a TelePresence Server to register to the Cisco VCS.
- **Cisco TelePresence Server Basic Setup for Cisco Unified CM Environment:** This section examines the configuration settings needed for a TelePresence Server to operate with the Cisco Unified CM.
- **Cisco TelePresence Server Conference Creation and Management:** This section explains how to create conferences on the Cisco TelePresence Server and explains the tools available to manage conferences.
- **Cisco TelePresence Server Troubleshooting:** This section examines logs available on a TelePresence Server that you can use to troubleshoot problems.

CHAPTER 15

Cisco TelePresence Server

The race for the best telepresence experience brought about much great advancement in the video telecommunications (VTC) industry. Cisco developed the Telepresence Interoperability Protocol (TIP) and made it open source. It is now widely used cross-vendor around the world. Cisco also developed the CTS 3000 series Immersive TelePresence Room Solution that sent other vendors scrambling to compete. Shortly after the CTS 3000 came out, TANDBERG developed the T3 Immersive Room Solution, and Polycom acquired a company that had an immersive room solution as well. With all these great multiscreen, multi-endpoint room solutions coming out, a chasm was created between the immersive telepresence solutions and the single-screen, single-endpoint products. That is what prompted TANDBERG to develop the TelePresence Server.

The TelePresence Server is a multipoint control unit (MCU) that understands the difference between single-screen and multiscreen systems. It also handles TIP autocollaboration. This one product revolutionized the VTC industry and paved the way for many more advancements, which everyone is still witnessing today. This might be the pinnacle product that prompted Cisco to purchase TANDBERG. This chapter covers how to install a Cisco TelePresence Server, configure the server to register to the VCS and interoperate with the Cisco Unified CM, create and manage conferences, and examine the logs available on the Cisco TelePresence Server that you can use to aid in troubleshooting call-related issues.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 15-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 15-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Cisco TelePresence Server Installation	1–2
Cisco TelePresence Server Basic Setup for Cisco VCS Registration	3
Cisco TelePresence Server Basic Setup for Cisco Unified CM Environment	4
Cisco TelePresence Server Conference Creation and Management	5
Cisco TelePresence Server Troubleshooting	6–7

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What is the baud rate that should be used when connecting to a Cisco TelePresence Server via a console cable?

   a. 9600
   b. 38400
   c. 96000
   d. 110200

2. What is the minimum limitation of ephemeral ports that can be configured on the Cisco TelePresence Server?

   a. 1000
   b. 2500
   c. 5000
   d. 52,535

3. Which of the following statements about registering the Cisco TelePresence Server to the Cisco VCS is true?

   a. All TelePresence Server products can register to the Cisco VCS using SIP/H.323.
   b. TelePresence Server products can only register to the Cisco VCS using SIP.
   c. TelePresence Server products can only register to the Cisco VCS using H.323.
   d. Some TelePresence Server products can only register to the Cisco VCS using SIP.

4. Which of the following options is available on Cisco TelePresence Servers in a Cisco VCS environment but not in a Cisco Unified CM environment?

   a. Ad hoc conferences
   b. SIP
   c. BFCP
   d. Rendezvous conferences

5. Which of the following options is available on Cisco TelePresence MCUs but not on the Cisco TelePresence Servers?

   a. Multisite
   b. BFCP
   c. Auto attendants
   d. Different layouts

6. Which of the following is not a tool that can be used for troubleshooting on the Cisco TelePresence Server?

   a. Audit log
   b. Event log
   c. Connectivity tool
   d. Status

7. What is the function of the API Clients feature on TelePresence Servers?

   a. Allows administrators to issue API commands from a menu option on the web interface
   b. Allows administrators to disable access to the API from the web interface
   c. Allows administrators to view API requests from the web interface
   d. Allows administrators to terminate API sessions of other users from the web interface

Foundation Topics

Cisco TelePresence Server Installation

The engineers and developers who designed and created the Cisco TelePresence Server were a culmination of product specialists who also helped develop the Cisco Video Communications Server (VCS) and the Cisco TelePresence MCU. Therefore, the interface of the Cisco TelePresence Server has the look and feel of the Cisco VCS. However, the underlining kernel is based on the Cisco TelePresence MCU products. The Cisco TelePresence Server uses the same method of installation as the Cisco TelePresence MCU. Because the Cisco TelePresence Server is also available as a blade or appliance-based server, initial installation differs slightly depending on the platform being used. Cisco TelePresence Server blade's network settings are configured through the Supervisory blade of the MSE 8000 blade chassis. This section focuses on how to configure an appliance Cisco TelePresence Server network settings.

On the front of the panel of the appliance TelePresence Server, there is a Console port. The cable needed to connect to this console port is an RS232-to-RJ-45 serial cable. Connect the RJ-45 connector of the cable to the Console interface of the TelePresence Server. Connect the RS232 connector on the cable to a PC. An RS232-to-USB converter may be needed if your computer does not have a serial port built-in. Open a terminal session like PuTTy. Change the connection type to Serial. Set the Serial line to the Com port the cable is connected to on the PC, and configure the remaining settings as follows:

- **Speed (baud):** 38400
- **Data bits:** 8
- **Stop bits:** 1
- **Parity:** None
- **Flow Control:** None

After the terminal session has been configured, start the session. On the Cisco TelePresence Server, connect the network cable to the LAN port on the front panel. Connect the power cable to the TelePresence Server, and the unit should begin the power-up process. This can be observed from the terminal session.

The Cisco TelePresence Server uses Dynamic Host Configuration Protocol (DHCP) by default. Best practice suggests that the IP settings should be changed to a static IP address. After the TelePresence Server has completed the boot process, a simple command can be issued from the terminal session to change these parameters. In the terminal session, enter the command **static** *ip-address subnet-mask default-gateway dns-address*, and then press the **Enter** key. Even though your organization may not use Domain Name System (DNS), something must still be entered into that field. You can either enter a public DNS address or use the default gateway address again. After the static IP address settings have been configured, the TelePresence Server needs to be rebooted to bind the network settings to the server. Type the command **shutdown**. The system will go through a shutdown process, but only the services will be stopped. When the interface receives the message "The

TelePresence Server has shut down," enter the command **boot**. This initiates a process where the TelePresence Server will shut down the rest of the way and reboot, this time using the new static IP address assigned to it. When the Cisco TelePresence Server has finished the reboot process, the administrator can web into the unit through a web browser.

The settings that need to be configured from the web interface to finalize the initial setup of the Cisco TelePresence Server are similar to the MCU, discussed in the preceding chapter. However, the look and feel of the web interface of the TelePresence Server is different, as are some of the menu options. Figure 15-1 shows the menus that will be available when an administrator logs in to the Cisco TelePresence Server.

Figure 15-1 *Cisco TelePresence Server Main Menus*

Notice in Figure 15-1 that although the look of the web interface is different from that of Cisco TelePresence MCU, the menu structure is very similar. To access the web interface, open a web browser and navigate to the IP address of the TelePresence Server. Log in with the username **admin** and leave the Password field blank. Navigate to **Network > Network Settings**, and under the Port A IP Status section verify that the correct IP address information is displayed. Scroll down to the Port A Ethernet Status section and verify that the **Duplex** is negotiated at **Full Duplex**.

Next, navigate to **Network > DNS**, and enter the hostname and domain for the TelePresence Server. Together these two settings make up the DNS A record as it would appear within the DNS server. A secondary DNS address can be entered at this time as well. The hostname is also the system name. This will appear in TMS after the TelePresence Server is added. Click the **Update DNS Configuration** button. Verify that the information is displayed correctly under the DNS Status section.

Key Topic

Navigate to **Network > Services**. Ensure that all the services you intend to use are enabled by checking the box beside the port number, and ensure that the port numbers match the ports used within your network. Default port numbers are displayed automatically. The TCP services available on the virtual TelePresence Server include HTTP, HTTPS, SIP (TCP), and Encrypted SIP (Transport Layer Security [TLS]). There is no H.323 support on the TelePresence Server 300 series or the virtual version. The UDP services available on the virtual TelePresence Server include only SIP (UDP). Under the Services menu of the TelePresence Server, there is also a section called Ephemeral Port Range. This allows administrators to define the minimum and maximum ports used for UDP media for all calls involving the TelePresence Server. The default minimum port is set to 45152 and can be changed to a minimum setting of 10000. The maximum port range is preset at the cap limit of 65535, which provides an ephemeral port range of roughly 15,000 ports. The maximum setting can be reduced so long as the range of ports does not drop below 5000 available ports. Reducing this range below 5000 ports could potentially affect conferencing functionality. If changes were made on the Services page, click the **Apply Changes** button to save the setting changes.

Because the admin account does not use a password by default, a password must be created to secure the Cisco TelePresence Server. Navigate to **Users > Users**. Click the blue **admin** account hyperlink. This will take you into the configuration page. Click the **Change Password** button, and enter a password in the New Password and Re-Enter Password sections. Click the **Change Password** button. This will change the password for the TelePresence Server. The initial setup of the Cisco TelePresence Server is now complete.

Cisco TelePresence Server Basic Setup for Cisco VCS Registration

Key Topic

On a Cisco TelePresence Server 7010 appliance or an 8710 blade, two operation modes can be configured. To configure the operation mode from the web interface, navigate to **Configuration > Operation Mode**. When the operation mode is set to **Remotely Managed**, the TelePresence Server is not registered to any call control device. Rather, the Cisco TelePresence Conductor manages its resources. When the operation mode is set to **Locally Managed**, the TelePresence Server can act independent of the Cisco TelePresence Conductor and register to the Cisco VCS or be trunked to the Cisco Unified Communications Manager (CM). The Cisco TelePresence Servers 300 series and virtual TelePresence Server act only in remotely managed mode, so this menu option does not appear on their web interface. They can only be used in conjunction with a Cisco TelePresence Conductor. Because discussion of the Cisco Conductor is beyond the scope of this book, this section and the next section focus on how to deploy a Cisco TelePresence Server 7010 appliance or an 8710 blade.

After the network settings have been configured and validated, the Cisco TelePresence Server can be configured for registration. The settings that need to be configured for registration vary depending on whether the TelePresence Server registers to the Cisco VCS or is trunked with the Cisco Unified CM. The TelePresence Server can register to the Cisco VCS using H.323/SIP (Session Initiation Protocol), but 300 series and virtual TelePresence Servers can only support SIP. Also, the Cisco Unified CM can only support SIP communication.

To register the Cisco TelePresence Server to the Cisco VCS, navigate to **Configuration > SIP Settings**. Change the following settings, and then click the **Apply Changes** button to save the changes:

- **Outbound Call Configuration:** Change from Call Direct to **Use Trunk**.
- **Outbound Address:** Enter the IP address or URL of the VCS to which you want the TelePresence Server to register.
- **Outbound Domain:** Only the domain used for SIP should be configured, not the full URI for the TelePresence Server.
- **Username:** If authentication is used on the call control server, such as the Cisco VCS, this username is used for authentication purposes. This field works in conjunction with the Password field.
- **Password:** If authentication is used on the call control server, such as the Cisco VCS, this password is used for authentication purposes. This field works in conjunction with the Username field.
- **Outbound Transport:** Select the protocol the TelePresence Server will use for outbound calls. The choices are TCP, UDP , or TLS. TLS can be used only if the encryption feature key is installed.
- **Advertise Dual IPv4/IPv6:** Select **User ANAT** if the TelePresence Server needs to support an IPv4/IPv6 mixed network environment.
- **Negotiate SRTP Using SDES:** The TelePresence Server supports the use of encryption with SIP. When encryption is in use with SIP, the audio and video media packets are encrypted using Secure Real-time Transport Protocol (SRTP). When using the SRTP, the default mechanism for exchanging keys is SIP Security Description (SDES). SDES exchanges keys in clear text, so it is a good idea to use SRTP in conjunction with a secure transport for call control messages. You can configure the TelePresence Server to also use Transport Layer Security (TLS), which is a secure transport mechanism that can be used for SIP call control messages. This setting can be configured as **For Secure Transport (TLS) Only** (which is the default setting) or **For All Transports**.

Cisco TelePresence Server Basic Setup for Cisco Unified CM Environment

The Cisco TelePresence Server can act as an ad hoc bridge on the Cisco Unified CM only when it is operating in remotely managed mode through the Cisco TelePresence Conductor. It is actually the Cisco TelePresence Conductor that is added to the Cisco Unified CM as a media resource. In a deployment in which the Cisco TelePresence server operates in conjunction with the Cisco Unified CM in locally managed mode, only rendezvous conferencing is available. There is no support for using the TelePresence Server as an ad hoc bridge on the Cisco Unified CM in locally managed mode. Therefore, the setup of the TelePresence Server is quite different from that of the Cisco TelePresence MCU as discussed in the preceding chapter. The settings that need to be configured on the Cisco Unified CM to communicate with the TelePresence Server are the same as with communication to the Cisco VCS. A trunk needs to be created on the Cisco Unified CM pointing to the Cisco TelePresence Server, with appropriate route patterns created for the trunk.

To create a SIP trunk on the Cisco Unified CM, log in through the web interface and navigate to **Device > Trunk**. Click the **Add New** button, select **SIP Trunk** from the Trunk Type drop-down list, click the **Next** button, and configure the appropriate settings. Exactly what you need to configure will depend on your collaboration environment and goes beyond the scope of this chapter. Figure 15-2 illustrates some of the settings that you can configure on the Cisco Unified CM trunk settings page.

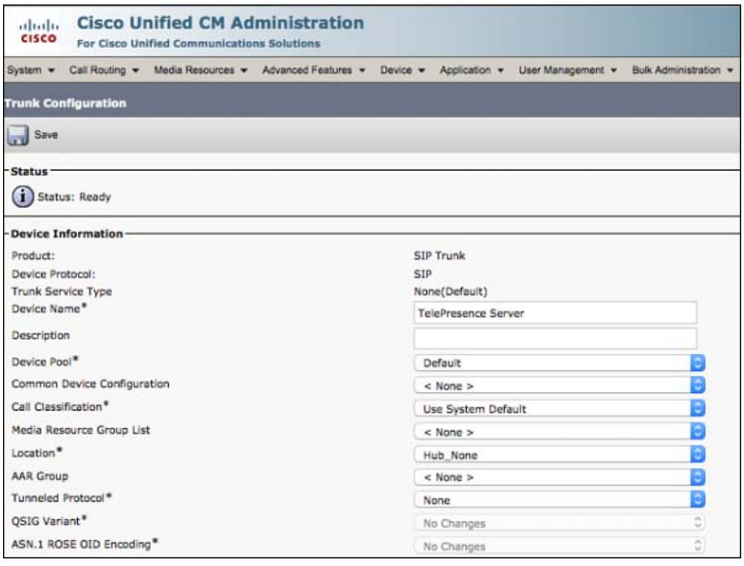


Figure 15-2 *Trunk Settings on the Cisco Unified CM*

After the trunk has been saved, route patterns can be created on the Cisco Unified CM. Route patterns determine when and where calls should be routed based on the aliases dialed. To configure the necessary route patterns, navigate to **Call Routing > Route Hunt > Route Pattern**. Click the **Add New** button and fill out the appropriate fields. As with SIP trunks, the fields that need to be configured depend on your collaboration environment, which goes beyond the scope of this chapter. Figure 15-3 shows some of the configuration settings available for route patterns on the Cisco Unified CM.

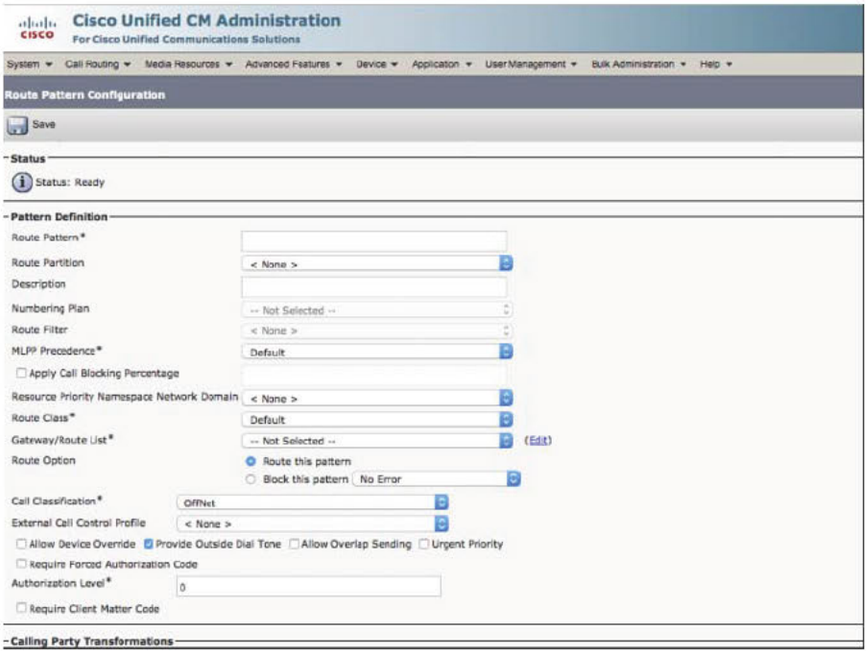


Figure 15-3 *Route Pattern Settings on the Cisco Unified CM*

Cisco TelePresence Server Conference Creation and Management

Key Topic

Once the Cisco TelePresence Server has either registered to the Cisco VCS or is trunked with the Cisco Unified CM, conferences can be configured. It is important to note that the Cisco TelePresence Server can be use as an ad hoc bridge in a Cisco VCS environment only without the use of the Cisco TelePresence Conductor and that there is not an auto attendant, or interactive voice response (IVR), function available on this device. It is also important to note that the Cisco TelePresence Server 300 series and the virtual TelePresence Server can only be used in conjunction with the Cisco Conductor. Discussion about the conductor is beyond the scope of this chapter. You can find more information on the Cisco TelePresence Conductor in the Cisco TelePresence Conductor Configuration Guides available at http://tinyurl.com/TelePConduct.

Conferences can be scheduled in advance on the Cisco TelePresence Server. On the web interface of the Cisco TelePresence Server, navigate to **Conferences >Add New Conference**. Configure the following fields, and then click the **Add New Conference** button when finished. Table 15-2, taken from the *Cisco TelePresence Server Administration Guide*, describes the conference configuration fields available on a Cisco TelePresence Server.

Key Topic

Table 15-2 TelePresence Server Conference Configuration Options

Field	Field Description
Name	The name of the conference.
Numeric ID	The unique identifier used for dialing in to the conference.
PIN	Enter the unique PIN for the conference.
Register Numeric ID with H.323 Gatekeeper	Whether to register the conference with the numeric ID as the H.323 ID.
Register Numeric ID with SIP registrar	Whether to register the conference with the numeric ID with the SIP registrar.
Conference Locked	Locks a conference.
Encryption	Whether encryption is optional or required for this conference.
Use One Table Mode When Appropriate	If your multiscreen endpoints support the one table feature, you can select whether to use one table mode automatically when the correct combination of endpoints or endpoint groups is in a conference (3 or 4 one table endpoints plus less than 6 other endpoints or endpoint groups). Options include Disabled and 4 Person Mode.
Content Channel	If enabled, the content is able to support an additional video stream, sent potentially to all connected endpoints, intended for showing content video. This content video is typically high-definition, low-frame-rate data such as a presentation formed of a set of slides. Such presentation data can be sourced by an endpoint specifically contributing a separate content video stream.
Automatic Gain Control	Controls the AGC setting for this conference. Options include Use Default, Disabled and Enabled.

Other settings can be configured when scheduling conferences, such as Port Limits and Lobby Settings and Scheduling settings. However, the basic settings represented in Table 15-2 are the basic settings that need to be configured on the Cisco TelePresence Server.

Conferences that are hosted by a Cisco TelePresence Server can be monitored through the TelePresence Server web interface. Navigating to **Conferences > Conferences** will display a list of all the conferences available on the Cisco TelePresence Server. From here, administrators can identify each conference by their unique name and conference ID. They can also see the status of the conference, whether it is Scheduled, Enabled, Active, Permanent, Inactive, or Completed. The difference between an enabled conference and an active conference is that an enabled conference is available for use but has no participants connected to it. An active conference has at least one participant that has joined the conference. If a conference lacks a numeric ID, or has a numeric ID but is not registered, it is considered disabled. A disabled conference can show up as active if a participant joins the conference. Such is true in a Cisco Unified CM environment.

Clicking a conference name will take you to a page that displays other conference status information. Information available includes the following:

- How many participants are connected to an active conference
- Whether the conference is registered to an H.323 gatekeeper or SIP registrar
- Whether the conference is locked
- Determined port limits set for this conference, and what they are
- Identify if this conference includes a content channel
- The status of all participants connected to the conference, if any
- If there were previous participants connected to this conference who disconnected, who they were is identified here as well

The controls available for administrators from the web interface management page includes the following:

- Adding participants to the conference
- Disconnecting a single participant
- Disconnecting all participants
- Sending a text message to one or all endpoints connected to the conference
- Expanding status information for individual participants
- Changing the layout of the conference

There are only two layout options available on the Cisco TelePresence Server, as follows:

- **Two participant mode:** Display up to two participants on each main monitor, allowing for six participants to be visible in full size on a three-screen immersive endpoint.
- **One table mode (also referred to as four participant mode).** Allows for 4 participants to be seen in full size on a single main monitor and up to 12 participants viewed on a three-screen immersive endpoint.

Cisco TelePresence Server Troubleshooting

Several tools are available on the Cisco TelePresence Server that you can use to troubleshoot issues, many of which are the same as or similar to the tools available on the Cisco Telepresence MCU. In addition to the status information discussed in the previous section, there is also an Event log, Protocols log, CDR (call detail record) log, and API Clients. Administrators can download diagnostic information and system logs. There is also a tool that can be used to test connectivity between the Cisco TelePresence Server and other devices.

Logs can be accessed on the TelePresence Server by navigating through the Logs menu. There are several logs available, each with its own unique function. The Event log provides basic event status for TelePresence Server operations. The events available in the Event log include info, warning, and error. The event capture filter can be used to change the level of information available in the Event log. The Protocols log is similar to the H.323/SIP log on the Cisco TelePresence MCU. The Protocols log allows administrators to take detailed

call traces on SIP, H.323, Binary Floor Control Protocol (BFCP), and eXtensive Conference Control Protocol (XCCP) communications. H.323 is not available in virtual and 300 series TelePresence Servers. This should not be enabled except at the time an issue needs to be traced to find the root cause. The information is stored locally on the TelePresence Server. Because this log contains a high level of information, it can fill up very quickly. If the log were to fill up, it would affect the performance of the TelePresence Server. This information can be stored on a remote server using the Syslog submenu. The event display filter controls the level of trace the Protocols log provides. The CDR log is a call detail record that shows all participant interaction with conferences on the TelePresence Server. The API Clients submenu can be used to show the 10 most recent application programming interface (API) clients that have made requests to the unit. Any clients in the list that have not made an API request in the past 5 minutes will be grayed out. Information provided under API Clients includes client IP, time since last request, last request method, last request user, and requests received since last reset. All of these logs can be downloaded in Extensible Markup Language (XML) format and can be manually deleted if they become too full.

Diagnostics information and system logs can be downloaded by navigating to **Status**, scrolling to the bottom of the page, and clicking the related hyperlink provided. This is generic information representing the whole TelePresence Server. If an endpoint is unable to call into a conference, it could be a network-related issue preventing connectivity between that endpoint and the TelePresence Server. There is a tool that enables administrators to test the connectivity to any other device within the network from the TelePresence Server. Navigate to **Network > Connectivity** to access this tool. In the box beside Remote Host, enter the IP address of the device you are testing connectivity to, and then click the **Test Connectivity** button. The TelePresence Server will run a **ping-route** to that device and display the information in the window to the right. Figure 15-4 shows the use of the network connectivity test tool on the Cisco TelePresence Server.

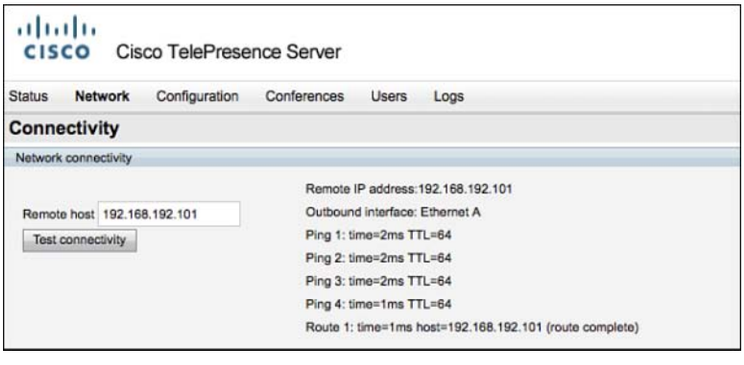


Figure 15-4 *Cisco TelePresence Server Network Connectivity Tool*

Summary

After completing this chapter, you should understand how the Cisco TelePresence MCU compares to the Cisco TelePresence Server. Although they share many similarities, there are also many differences in menu options and functions. This chapter provided a basic understanding of how the Cisco TelePresence Server is installed and operates and the native tools available for troubleshooting within your environment.

This chapter examined how to install an appliance Cisco TelePresence Server. Once the TelePresence Server is installed, configuration settings need to be set up to register to the Cisco VCS, which supports both H.323 and SIP registration on some TelePresence Server products, but only SIP on others. A unique set of configuration settings must be configured on the Cisco Unified CM for rendezvous conferences on the TelePresence Server. This chapter also covered how to create and configure scheduled conferences and how to manage conferences after they have started. This chapter also assessed different logs and tools available on the Cisco TelePresence Server that you can use to troubleshoot issues as they develop.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 15-3 lists a reference of these key topics and the page numbers on which each is found.

Table 15-3 Key Topics for Chapter 15

Key Topic Element	Description	Page Number
Bulleted list	Know the settings on the Cisco TelePresence Server to establish a serial connection.	338
Paragraph	Understand the purpose and limitations for ephemeral ports on the Cisco TelePresence Server.	340
Paragraph	Understand what TelePresence Server environments can only support SIP.	340
Paragraph	Understand what environments support ad hoc conferencing with the Cisco TelePresence Server.	341
Paragraph	Understand the lack of an auto attendant function on Cisco TelePresence Servers	343
Table 15-2	Know how to configure conferences on the Cisco TelePresence Server using the web interface.	344
Paragraph	Ability to list the different troubleshooting tools available on the Cisco TelePresence Server.	345
Paragraph	Identify what the API Clients option is used for on the Cisco TelePresence Server and how to navigate to it.	345

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

VTC, API, TLS, SDES, SRTP, AGC, one table mode

This page intentionally left blank

This chapter covers the following topics:

- **TMS Overview:** This section explains the purpose of TMS and provides an overview of the main functions TMS can perform.
- **Adding Systems to TMS:** This section explains how to add systems to TMS, how to view tickets associated with the added systems, and how to change settings on those systems from TMS.
- **Scheduling Conferences Using TMS:** This section covers how to schedule conferences on TMS using the Booking menu and using the Smart Scheduler tool.
- **Monitoring Conferences Using TMS:** This section explains how to monitor conferences from TMS using the Monitoring Center.
- **TMS Reporting:** This section briefly overviews the reporting options available on TMS.

Cisco TelePresence Management Suite

Up to this point, this book has focused primarily on endpoints. As to the maintenance and management of a Cisco collaboration network, every task can be performed either from the Cisco Unified Communications Manager (CM) or natively on the endpoint. For example, in a Cisco Unified CM-centric environment, the TFTP server pushing a current firmware load to the endpoint can upgrade most endpoints registered. The exception to this rule is TC software-based endpoints, which would have to be upgraded manually on the endpoint itself. Other tasks, such as configuration backup and restore, can be performed natively on the endpoint. Multipoint conferences can be scheduled natively on a Cisco TelePresence MCU or a Cisco TelePresence Server, or ad hoc conferences can be created on the fly. So it would seem that so long as an organization has some sort of call control server, a multipoint control unit (MCU) and some endpoints that nothing else is needed for daily operation and support of the collaboration solution. This assumption is in fact true. However, as an organization grows and the collaboration solution expands, these remedial tasks can become quite cumbersome. Therefore, there is a tool that can be used to simplify how a Cisco collaboration solution is managed. This tool is known as the Cisco TelePresence Management Suite (TMS). TMS brings minimal functionality to the table that cannot already be performed on another device. The advantage of using TMS is its capability to streamline and simplify the daily tasks of using and managing a Cisco collaboration network all from a single, easy-to-use web interface.

This chapter is not intended to give an exhaustive explanation of all the tasks TMS is able to perform. Instead, this chapter introduces a few of the most common tasks for which TMS is used. Those tasks include how to add systems to TMS, how to view open tickets on those systems, how to schedule and manage conferences from TMS, and an overview some of the reporting tools available on TMS.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 16-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 16-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
TMS Overview	1–2
Adding Systems to TMS	3–6
Scheduling Conferences Using TMS	7–8
Monitoring Conferences Using TMS	9
TMS Reporting	10

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What port does TMS use for LDAP integration?
   - **a.** 80
   - **b.** 161
   - **c.** 389
   - **d.** 443
2. Which applet is used to allow users to schedule conferences through Outlook?
   - **a.** TMSMO
   - **b.** Outlook
   - **c.** TMSPE
   - **d.** TMSXE
3. What protocol does TMS use to manage systems?
   - **a.** HTTP
   - **b.** SNMP
   - **c.** TFTP
   - **d.** LDAP
4. Which of the following endpoints can TMS not manage?
   - **a.** DX650
   - **b.** CTS500
   - **c.** MX700
   - **d.** SX10

5. Which of the following is an MCU that TMS can manage?

   a. Cisco Unified Communications Manager
   b. Cisco Video Communications Server
   c. Cisco TelePresence Server
   d. Cisco TelePresence Content Server

6. Which statement below is true for tickets on TMS?

   a. Tickets can be ignored or acknowledged.
   b. Tickets can be deleted or acknowledged.
   c. Tickets can be deleted or ignored.
   d. Tickets can only be viewed.

7. Which of the following is a conference type that allows users to join scheduled conferences when they are ready?

   a. Automatic Connect
   b. One Button To Push
   c. Manual Connect
   d. Reservation

8. Which tool can be used by nontechnical users to schedule conferences on TMS?

   a. TMS Scheduler
   b. TMS Booking Scheduler
   c. TMS Smart Scheduler
   d. TMS Easy Scheduler

9. What does TMS use for managing conferences in the Conference Control Center?

   a. IIS
   b. .NET
   c. SNMP
   d. Java

10. What report on TMS shows statistics reports on network and bandwidth usage?

    a. Network
    b. System
    c. Conference
    d. Call detail record

Foundation Topics

TMS Overview

As mentioned in the chapter introduction, Cisco TMS offers complete control and management of telepresence conferencing, infrastructure, and endpoints. Cisco TMS will increase the value of your collaboration conferencing network and simplify the daily management tasks by adding intelligence, diagnostics, and functionality to enhance your video network components. TMS provides management, deployment, and scheduling of the entire video network, including many Cisco call control, MCU, and gateway and endpoint devices, in addition to third-part devices providing the broadest multivendor support in the industry. TMS simplifies network management of TelePresence devices through built-in tools, such as automatic software updates with release keys generation, a built-in ticketing server, event notification through e-mail integration, and much more. Phonebooks have already been discussed in a previous chapter but warrant mentioning again. TMS has the ability to access and support local phonebooks that exist on endpoints and provision global and centralized phonebooks across the enterprise. TMS has native scheduling functionality; a built-in scheduling tool called Smart Scheduler; and the broadest range of support for third-party scheduling applications, such as Microsoft Outlook Exchange and Domino Lotus Notes. Cisco TMS ensures reliability and optimizes network use through an integrated intelligent call-routing engine.

TMS is an application that operates on a Microsoft Windows Server platform. The server resides in the data center, and TMS is used to manage the whole video network from this location. TMS can manage the video network both within and outside the firewall if the appropriate ports have been opened. Table 16-2 identifies the ports TMS uses within an enterprise for all operations.

Key Topic

Table 16-2 Ports Used by TMS

Service	Protocol	Port	Direction (Relative to TMS)	
			IN	Out
HTTP	TCP	80	x	x
HTTPS	TCP	443	x	x
Telnet	TCP	23		x
Telnet Chal.	TCP	57		x
Telnet PLCM	TCP	24		x
FTP	TCP	20, 21		x
SNMP	UDP	161	x	x
SNMP traps	UDP	162	x	x
SMTP	TCP	25		x
LDAP	TCP	389	x	x

Service	Protocol	Port	Direction (Relative to TMS)	
			IN	Out
TMS Agent	TCP	8989	x	x
Polycom GAB	TCP	3361	x	
Polycom	TCP	3601		x
Polycom	TCP	5001		x
TMS Agent Admin	TCP	4444	x	x

Cisco recommends using Microsoft Windows Server 2012 R2 64 bit as the platform for installing TMS software Version 14.4.1 or higher. Full details of the operating systems that are supported can be found in the *Cisco TelePresence Management Suite Installation and Getting Started Guide*. TMS cannot be installed until a SQL database is present either on the Windows Server or somewhere within the network accessible from Cisco TMS. You can install express editions of SQL Server free of charge. Cisco recommends using Microsoft SQL Server 2012 for new installations. Before installing or upgrading Cisco TMS, always check the current release notes and installation guide. TMS is accessible through a web interface using the Microsoft Internet Information Services (IIS). IIS operates on the Microsoft .NET platform. Both of these need to be installed on the Windows Server before TMS can be installed. Cisco recommends using IIS Version 8 or later and Microsoft .NET 4.5 or later. When all these components are in place, the TMS installation wizard can be started.

Key Topic

After TMS has been installed, two more optional components can be installed on the Windows server that enhance the functionality of TMS. TMS Provisioning Extension (TMSPE) is required for the Smart Scheduler tool to be used. This option also allows for devices to be provisioned through TMS, such as Jabber Video for TelePresence clients, and for TMS to provision FindMe templates to the Cisco Video Communications Server (VCS). The other optional application that can be installed on the Windows server is the TMS Exchange Integration (TMSXE). This allows TMS to be integrated with Microsoft Exchange servers so that conferences can be scheduled through Outlook clients on employee computers. Note that mail integration with TMS can be performed without the TMSXE application.

After TMS has been installed, the web pages can be accessed by navigating to the IP address or URL of the Windows server followed by /tms (for example, navigate to **http://192.168.176.20/tms**). A Windows authentication box will pop up on your screen. Log in using your user credentials, and the TMS Portal page will load. The TMS Portal gives a quick overview of the functionality that TMS offers and includes the following sections. The Systems section provides a summary of the different types of systems that are managed by Cisco TMS. A blue hyperlink will appear when there is one of more of each different system type that TMS is managing. The Systems Sorted by Ticket Level section shows the list of open tickets, which are grouped by ticket level. These tickets can be viewed by selecting the blue hyperlink made available if there are any tickets open. The Conferences and Reservations section provides a list of the conferences and reservations that are scheduled, active, finished, and requested for the day. The System Usage section is a graphical representation of scheduled and total conferences made involving devices TMS is managing.

TMS will view any call, whether it is point to point or multipoint, as a conference. The blue area in the system usage graph represents the number of endpoints that have been involved in calls throughout the day. Of all the active calls throughout the day, a green line represents the number of booked endpoints. Figure 16-1 shows the Portal page on Cisco TMS.

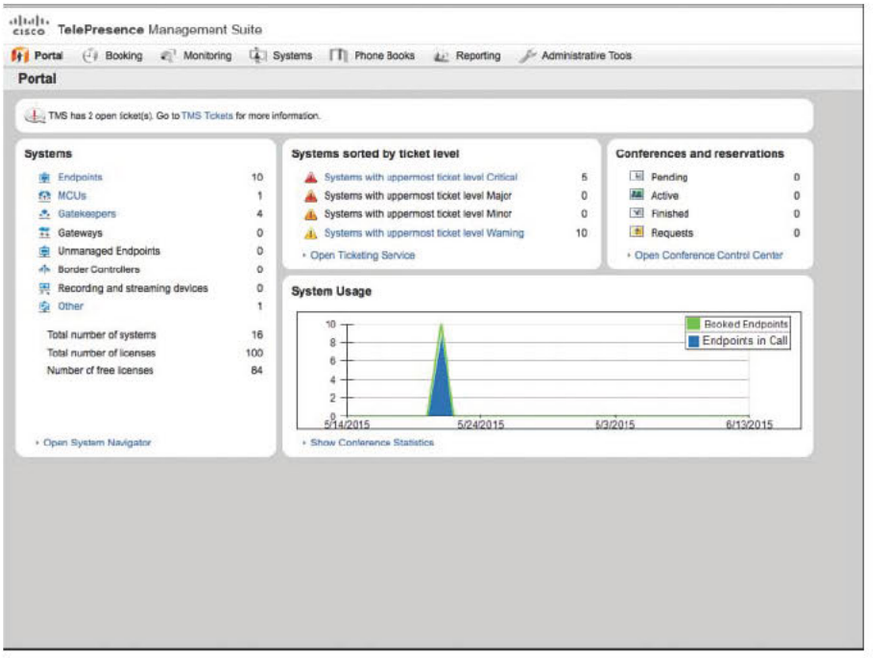


Figure 16-1 *Cisco TMS Portal Page*

Adding Systems to TMS

Key Topic

After TMS has been installed, all initial configuration settings have been configured, and all services are running, TMS can be used to manage the entire collaboration network. For TMS to manage a device, that device must be added to TMS. TMS uses Simple Network Management Protocol (SNMP) to discover and manage devices; therefore, SNMP must be turned on for each device. There is an exception that allows systems to be added to TMS without SNMP being turned on, but TMS cannot fully manage those systems. In the TMS solution, Cisco TelePresence TC software-based endpoints can be registered to the Cisco VCS or to the Cisco Unified CM. When endpoints are registered to the Cisco VCS, endpoints can be added to TMS directly. Then, when TMS is used to schedule conferences, a TMS administrator can add these endpoints to the conference. If endpoints are registered to Cisco Unified CM, they must be provisioned on the Cisco Unified CM before Cisco TMS can import them for scheduling. After the Cisco Unified CM has been added to TMS, there is an option to add endpoints registered to the Cisco Unified CM to TMS. Note that endpoints added to TMS from the Cisco Unified CM cannot be fully managed by TMS, but they can be added to scheduled conferences. Also, there are a lot of endpoints the Cisco Unified CM supports for registration that TMS will not import, such as the DX series endpoints.

TMS can provision the Cisco TelePresence MCU and Cisco TelePresence Server as well. Either of these products can be leveraged when conferences are scheduled on TMS, along with the multisite feature on endpoints, the Cisco Conductor, and third-party MCUs. TMS will decide which product to used based on the number of endpoints added to a conference, the types of endpoints added, and the number of ports available on different MCU products. There is an advanced Conference configuration setting on TMS that influences how TMS makes this decision, called External MCU Usage in Routing. To verify or change this setting, navigate to **Administrative Tools > Configuration > Conference Settings** and scroll down to the Advanced section at the bottom of the page. The External MCU Usage in Routing parameter contains the following options: **Always** will schedule an MCU in every scheduled call, even if only two endpoints are scheduled to communicate. Therefore, there is another setting called **Always Except Point to Point**. This setting will always include an MCU in scheduled conferences except for point-to-point scheduled calls. The Multisite option will never be used when **Always** or **Always Except Point to Point** are configured. If an administrator wants to use multisite whenever possible to preserve MCU resources, then there is a third setting that must be selected under this menu option. **Only If Needed** uses the multisite option on one of the scheduled endpoints whenever conferences are scheduled with few enough endpoints that multisite can support all the participants. If multisite cannot be used to support the conference for any reason, TMS will select an MCU to host the call. Figure 16-2 show these External MCU Usage in Routing settings and other options on the Cisco TMS.

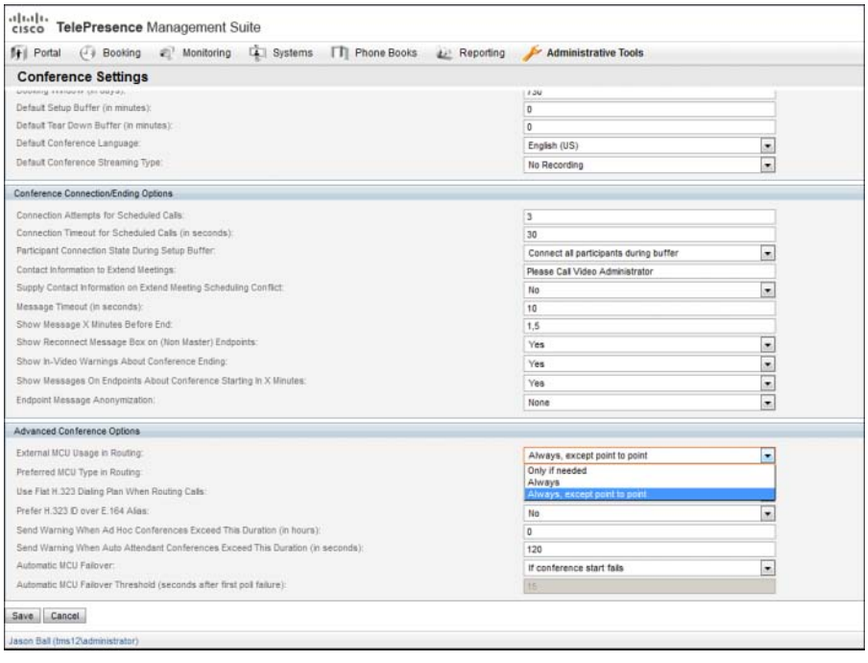


Figure 16-2 *External MCU Usage in Routing Setting on TMS*

Before conferences can be scheduled on TMS, endpoints and MCUs must be added to TMS so that it can manage them. Before you begin adding systems to TMS, it is recommended to first create folders. The structure of this tree hierarchy will greatly impact every other function performed on TMS. Folders and systems are added to TMS under the **System > Navigator** menu. In the Folder View section, select the folder within which you will create your various subfolders. Click the **New Folder** button. When the New Folder window displays, enter a name for the folder you are creating and click the **Save** button. This process can be repeated to create all the folders and subfolders needed to represent your corporation. Figure 16-3 shows how to add folders in TMS.

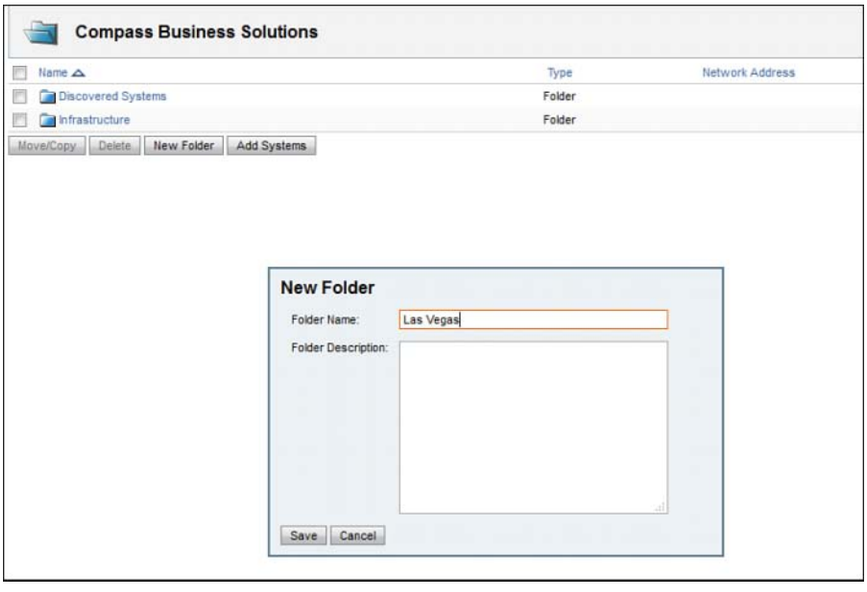


Figure 16-3 *Adding Folders in TMS*

After all the folders have been created, select a folder that you want to add devices to and click the **Add Systems** button. There are various ways devices can be added to TMS. For simplicity, this section only discusses how to add systems to TMS using the Add by Address tab. In the box under the Specify Systems by IP Address or DNS Names section, enter the IP address or URI of the systems you want to add. Multiple addresses can be added here using either a comma between them or a hyphen to represent a range of IP addresses. Expand the **Advanced Settings** section and enter the username and password of the systems you are adding to TMS. Click the **Next** button at the bottom of the page to start the system discovery process on TMS. Figure 16-4 shows how to add systems to TMS for TMS to manage them.

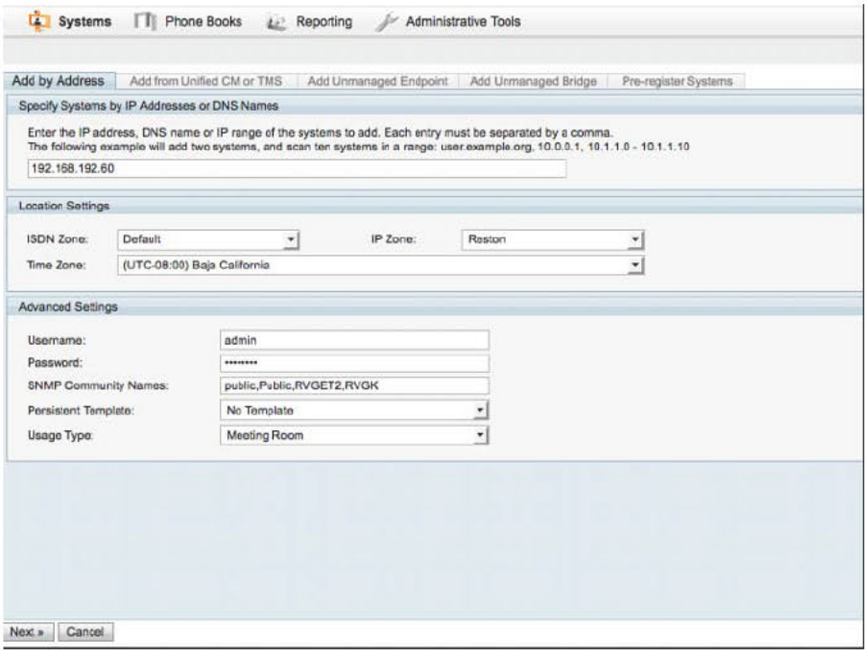


Figure 16-4 *Adding Systems to TMS*

Once the devices are added to TMS, the device settings can be seen and modified as needed. When you choose a system from Folder view, Cisco TMS Navigator displays a summary of the system. The summary sections include Tickets, Settings, Service Contract, and This Week's Bookings. You can use different tabs to verify and change settings on the device added. These tabs include Settings, Call Status, Phone Book, Connection, Permissions, and Logs. TMS Navigator only adds a Phone Book tab when the system that has been added in TMS is fully managed by TMS. This system must be accessible via the Web. On fully managed systems, Cisco TMS can provision different phonebook sources and manage many additional things, such as upgrading the endpoint.

Key Topic

Although selecting a device under **System > Navigator** will display open tickets on one particular system, there is a Ticketing Service page within TMS that can be used to view and manage open tickets on all devices that have been added to TMS. To access this ticketing service, navigate to **Systems > Ticketing Service**. For each error that the Cisco TMS discovers on the system, a new ticket is opened and associated with the system. The ticket is given a ticket ID, a description, and a severity level. Different sort options for displaying the tickets are available including Ticket Severity and Ticket Type. Ticket error levels are configurable by the system administrator. Open tickets cannot be deleted. They can either be acknowledged or be ignored.

Scheduling Conferences Using TMS

Once endpoints and MCUs have been added to TMS for management, conferences can be scheduled. There are two ways to schedule conferences from TMS. Users and administrators can access the Smart Scheduler tool, or TMS administrators can access the Booking menu from the TMS web interface. To schedule a conference using the Booking menu, navigate to **Booking > New Conference**. There are three sections displayed on the page that will open. The Basic Settings section contains all the basic configuration settings required for conferences to be scheduled. The Advanced Settings section contains certain advanced configuration settings that are not required but allow administrators to employ enhanced control when scheduling conferences. The third section is a series of tabbed menu options. Initially, there will only be two tabs: Participants and Conference Information. The options that exist will change as endpoints, and potentially MCUs, are added to the conference. Figure 16-5 shows some of the Booking options available through Cisco TMS.

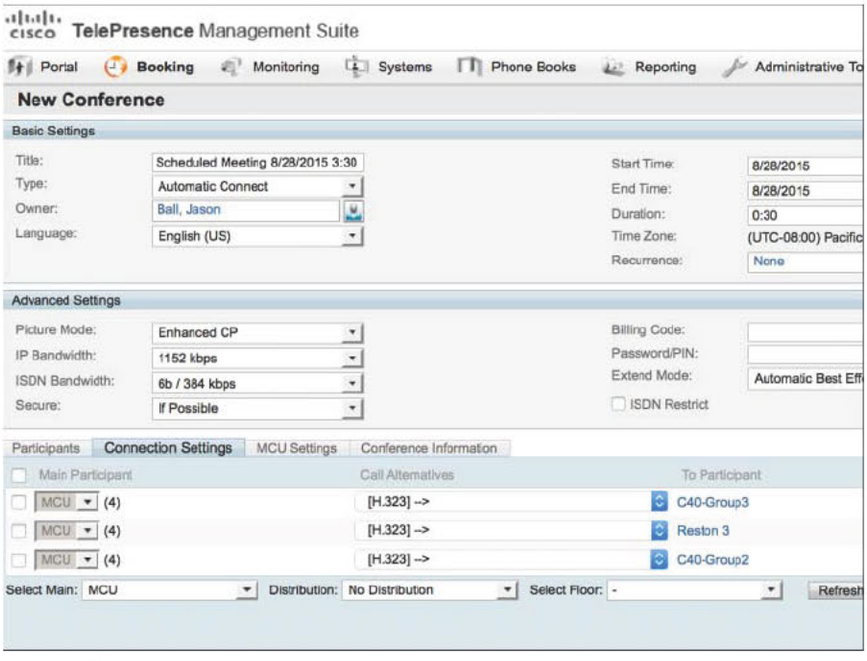


Figure 16-5 *Booking Option Through Cisco TMS*

Key Topic

As Figure 16-5 illustrates, the first section, Basic Settings, is broken down into the following fields. The Title of the conference is populated with a name created by a template. The title can be changed at any time. Type is a drop-down menu that contains the following five options:

- **Automatic Connect:** Connect all the participants.
- **One Button to Push:** Dial-in information will be pushed to supported endpoints.
- **Manual Connect:** The VC-Master endpoint will be prompted to begin the call.

- **No Connect:** Reserves the rooms and generates call route but does not connect.
- **Reservation:** Reserves the rooms but does not initiate or generate call route. Ports on the Cisco TelePresence MCU will be reserved for conference.

Owner is the default owner of the conference. This is determined by the administrator account used to log in to TMS. The owner of a conference can be changed, allowing conference creators to generate scheduled conferences on behalf of someone else. Start Time allows administrators to set the start date and time of conference. By default, the start date and time will always be the date and time the Booking menu was opened. Conferences can be scheduled to start immediately or for any time in the future. Similarly, End Time allows administrators to set the end date and time for scheduled conferences. The end time will always default to 30 minutes after the start time because the default conference duration is set to 30 minutes. The end time can be changed to any variation of time from the start time. Duration allows administrators to set the length of time allotted to the scheduled conference. As it has already been mentioned, the default duration is 30 minutes. Clicking on the **Recurrence** button will open a new window. If you want the conference being scheduled to occur at different points in the future, recurrence settings can be configured. Recurrence Pattern allow the choice of Daily, Weekly, or Monthly. Range of Recurrence offers choices of when the recurrences should cease.

The Advanced Settings parameters on the New Conference page include several options:

- The **Picture Mode** drop-down menu allows administrators to choose from one of the three "view modes" discussed in Chapter 13, "Cisco Multipoint Solution." The view modes are Continuous Presence, Voice Switched, and Enhanced CP.
- **IP Bandwidth** is not a bandwidth limitation, though it effectively operates as though it is a limit. Because TMS controls either the MCU calling out to the endpoints, or the endpoint dialing into the MCU, this setting determines the bandwidth rate that will be used. The range is from 64 kbps to 6144 kbps. If a participant were to dial in to the MCU manually, any bandwidth rate could be used.
- **ISDN Bandwidth** is not a limitation either. Once upon a time, most endpoints could support both ISDN and IP communication protocols natively. Therefore, TMS could be used to schedule ISDN calls using IP to communicate with the endpoint. This setting allows administrators to set the number of B channels followed by the bandwidth in kbps.
- The **Secure** drop-down menu allows for encryption to be enforced if necessary for all participating devices scheduled in this conference. The options are No, Yes, and If Possible.
- **Billing Code** is a feature that controlled a billing code setting native on MXP endpoints. Though these endpoints are end of sale, this feature still exists in TMS.
- **PIN** will protect conferences from unwanted participants for joining. Any participants who attempt to dial in to a conference that is PIN protected will be prompted to enter the PIN before they are allowed to join. If the MCU dials out to a participant, the PIN protection will not prevent the call from connecting.

- **Extend Mode** is a setting that allows conference times to be extended if the conference has run its length and participants still need more time to communicate. This drop-down menu offers three settings. Off prevents meetings from automatically extending. Endpoint Prompt displays an "Extend Meeting" message on compatible endpoints both 5 minutes and 1 minute before the end time of the conference. Automatic Best Effort enables the automatic extension of scheduled conferences by 15 minutes up to a maximum of 16 times in a single conference.

Click the **Add Participants** button to add participants to the conference. A pop-up window will open, so be sure to either turn off pop-up blocker or add an exception for this pop-up window to allow it to open. From the Add Participants window, you can add the conference participants using the different tabs. Figure 16-6 shows the different tabs available from the Add Participants window.

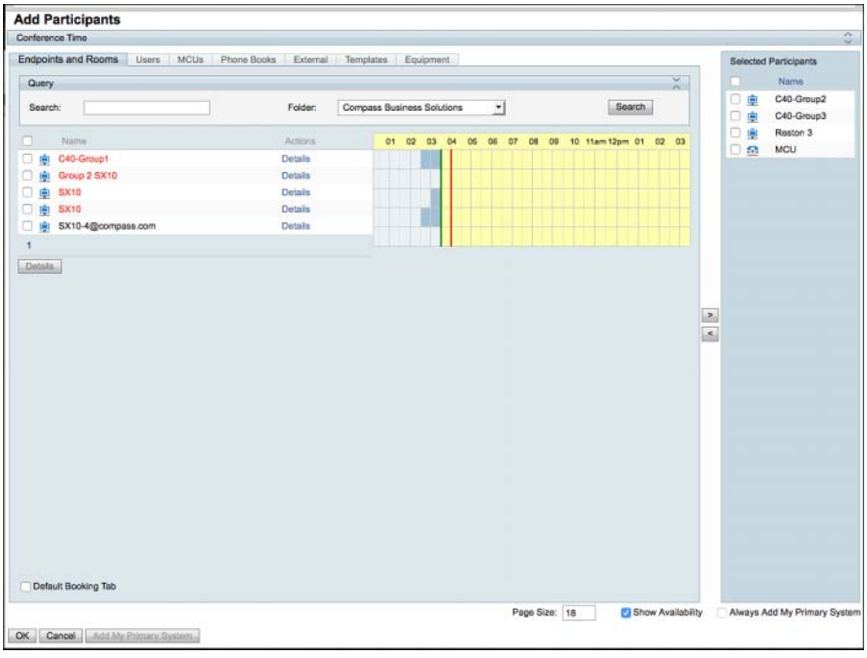


Figure 16-6 *Add Participant Window for Conference Creation on TMS*

The Last Used tab allows administrators to add participants from previous bookings. The Endpoints and Rooms tab allows endpoints and rooms that are managed by Cisco TMS to be added to conferences. The Users tab allows adding users who possess accounts within TMS. If a user has an endpoint associated with his or her account, that endpoint will be added to the conference. The users added through this method will automatically receive an e-mail confirmation that they have been scheduled for a conference at their e-mail account listed in their user account. MCUs allows administrators to add MCUs that are managed by TMS. It is not necessary to add an MCU to a scheduled conference because TMS will select the best option for you based on the External MCU Usage in Routing setting discussed in the previous section. However, if an administration wants to select a specific MCU, this

tab allows that option. The Phone Books tab allows participants to be added from TMS phonebook entries. If an administrator wants to add a participant who was located outside of an organizations network, the External tab should be used. From here, an alias can be added as a dial-out participant, where the MCU will dial their alias at the time of the conference. Alternatively, they can be added as a dial-in participant, which will require intended participants receive the conference confirmation information so that they have the dial-in credentials. Templates makes it possible to control how unmanaged systems are added to a conference. This tab is an advanced feature and should be hidden for users who are not using it. Equipment allows for the adding of other peripheral equipment that is managed by Cisco TMS, such as an ISDN gateway or a TelePresence Content Server (TCS) for recording the conference.

To add participants from any of these tabs, check the boxes to the left of the participant or endpoint name. If participants or devices are going to be added from multiple tabs, caret (>) the selected participants to the column on the right before changing tabs; otherwise, the participants selected will be lost. Click the **OK** button to save the selections. This will close the pop-up window and return you to the previous conference creation page. The participant should be listed at the bottom of this page under the Participants tab. There should now be four tabs listed in this bottom section, as follows:

- **Participants:** Check the availability of participants and add them to a conference. Any participant listed in red is already booked for the time the conference is set.
- **Connection Settings:** Contains information on how the call will be set up. The MCU or endpoint that multisite will be used on will be listed in the Main Participant section. All other participants will be listed in the To Participant section. Between these two sections is the Call Alternatives section. This will show the protocol that will be used to place the call and the direction the call will be connected. This setting can be changed on a participant-by-participant basis. The Dial String section lists the alias that will be used to connect the call. Other sections that can be configured are Bandwidth, Mute, and Actions.
- **MCU Settings:** This tab is only available if an MCU is being used to connect the calls. All the settings in this tab are reflective of the global conference settings. However, administrators can change these settings on a per-conference basis before scheduling the conference.
- **Conference Information:** This tab allows administrators to add e-mail addresses where the conference booking details can be mailed to. The options within this tab include Send E-mail To, E-mail Message, Conference Notes, and Reference Name.

After you have verified conference settings, click the **Save Conference** button to save the changes. The conference details will be displayed on the following page. These same conference details will be e-mailed to any participants added to the conference who have an account in TMS, and any participants whose e-mail address was added under the Conference Information tab.

Key Topic

Conferences can also be scheduled on TMS by using a built-in tool called Smart Scheduler. TMS Smart Scheduler is available on TMS as of Version 14.3, replacing its predecessor TMS Scheduler. It can be accessed by either clicking the small square icon in the top-right corner of the web interface or by navigating in a browser window directly to the path

https://<*TMS_IP_Address*>/tmsagent/tmsportal/?locale=en _ US#scheduler. This path is not commonly used and may vary based on deployment. The address of the Cisco TMS Smart Scheduler is usually provided through a specific DNS-based URL (for example, http://tms-scheduler.company.com, or the URL **https://<*TMS_IP_Address*>/tms/booking** expands to the longer URL shown earlier). Follow these steps to schedule a conference using Smart Scheduler:

Step 1. Click **New Meeting.**

Step 2. Under the Meeting Details section, you can change the title and start and end dates and times. In addition to Meeting Details, there are three menu sections: TelePresence, Recurrence, and Additional Settings. The section on the right side of the screen allows you to add participants and rooms. The TelePresence section shows which participants have been added to the conference. If CMR Hybrid is being used, there will be an Add WebEx option under the TelePresence section as well.

Step 3. After checking the settings, click the Save button to confirm the booking of the conference.

Figure 16-7 shows what the TMS Smart Scheduler tool will look like.

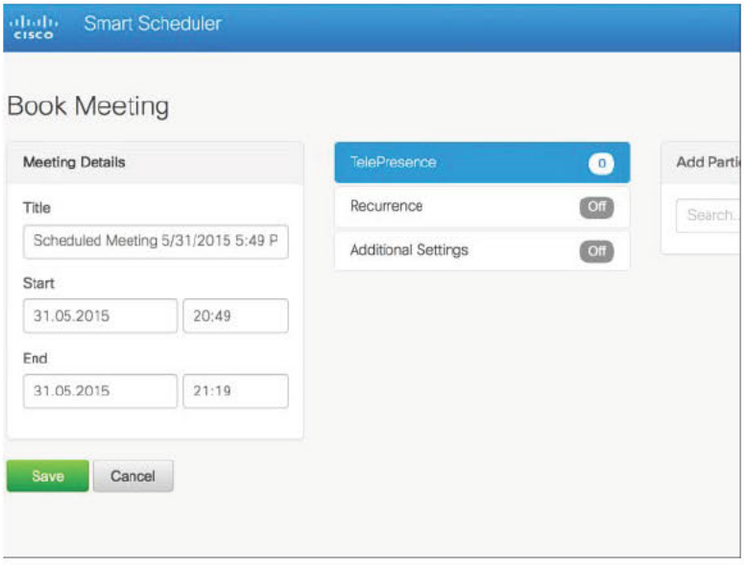


Figure 16-7 *TMS Smart Scheduler*

Managing Conferences Using TMS

Key Topic

After conferences have been scheduled, they can be monitored from TMS. To monitor conferences in Cisco TMS, navigate to **Monitoring > Conference Control Center**. The Conference Control Center uses Java for dynamic information relative to the conference.

Java requires administrators to log in again. Use the same credentials you would use to log in to TMS. The Conference Control Center gives you total control over the active conference. On the Search frame, you can locate the conference that you would like to control. After you have selected the conference, voluminous conference-related information will be displayed. From the Participants tab, you can view a list of participants, including a preview of information about them, and control the picture mode. Use the Participant Status, Event Log, and Graphical View tabs for additional control of the conference. Selecting a participant will display a list of conference management tools that can be used for various purposes. Some of the controls include dial a participant, disconnect a participant, mute the audio and video, allow a participant to occupy the main screen of the conference, and send a text message. Most of the conference control functions available natively on the MCU can be performed from the Conference Control Center on TMS. Figure 16-8 shows how the Conference Control Center would appear to an administrator.

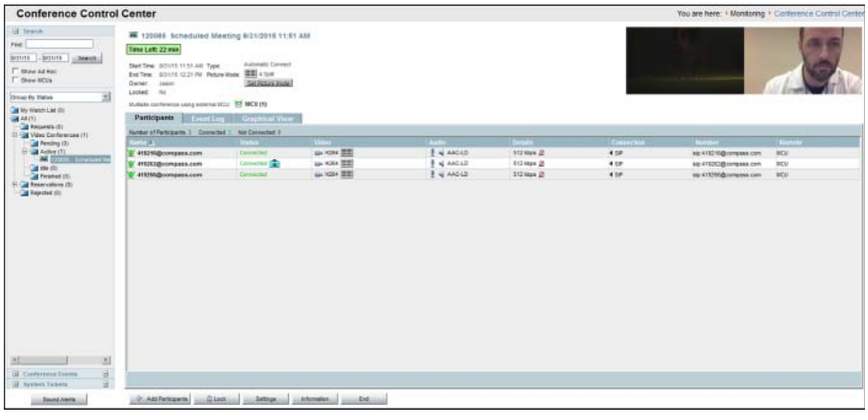


Figure 16-8 *Cisco TMS Conference Control Center*

Note TMS is very particular about what version of Java is supported per the version of TMS running within a customer network. When accessing the Conference Control Center on TMS, if Java indicates an error, or denies access to the Conference Control Center, consult the *Cisco TMS Administration Guide* for the appropriate version of Java that should be used with TMS.

TMS Reporting

The Cisco TMS reporting tool is a powerful and robust tool. TMS sources data from all the devices it manages to populate the reports that are generated automatically. To view system reports in Cisco TMS, move your mouse over the **Reporting** tab. A drop-down menu of all the reports available in TMS will be listed. Figure 16-9 illustrates the conference statistics displayed from the TMS Reporting menu.

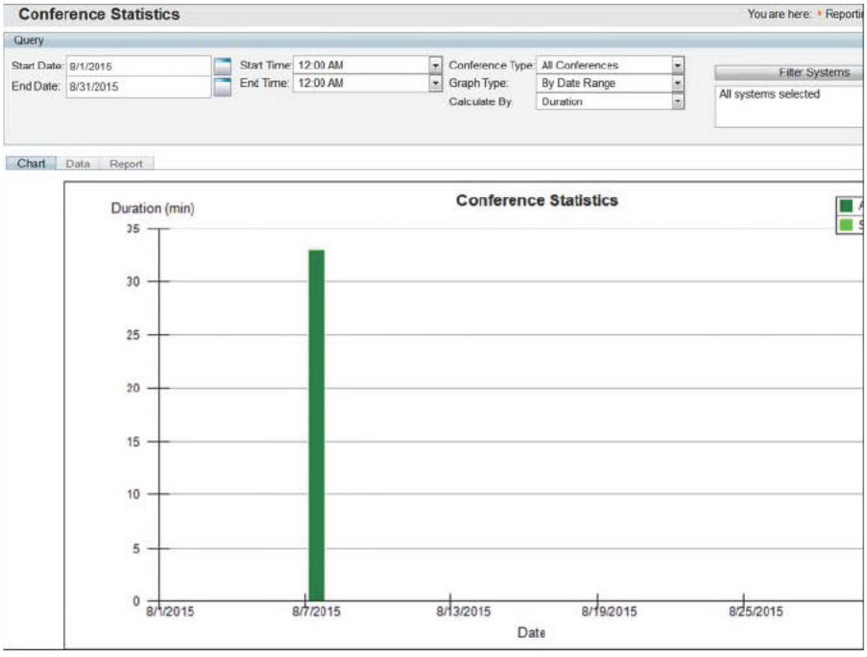


Figure 16-9 *Conference Statistics Displayed from the TMS Reporting Menu*

Each report will have a Chart, Data, and Report view tab. The Data tab gives you the option to export data in an Excel format. Under the Report tab, you can export reports as a PDF file. The Query section at the top of the page enables you to set the range of captured data using multiple filter systems options. The options available always include Start Date, End Date, Start Time, and End Time. Other options may include Call Protocol, Conference Type, Graph Type, Calculated By, and many more depending on the reporting purpose. Each report could measure data based on all systems, or a Filer Systems option could be used to target specific systems. Each report that has been modified can be saved as a template. At the bottom of the list is a Reporting Template option that can be used to view and modify templates you created for TMS reports. From here, the reporting template can be run or edited. Table 16-3 identifies all the menus and submenus in the reporting section of TMS, along with a description of each report's purpose.

Key Topic

Table 16-3 Reports Available on Cisco TMS

Main Menu Option	Submenu Options	Purpose
Bridge Utilization		The Bridge Utilization page contains reporting information on how much Cisco TMS-managed bridges are being used. The data is gathered from direct-managed TelePresence Servers and TelePresence MCUs only.

Main Menu Option	Submenu Options	Purpose
Call Detail Records	All Endpoints and MCUs Endpoints MCUs Content server Gateway Gatekeeper and VCS User CDR	Tracks the frequency and duration of calls in your TelePresence deployment.
Billing Code Statistics		Shows which billing codes are applied to conferences.
Conferences	Conference Statistics Resources Events Scheduling Interface Bridging Methods	Tracks conferences per user, type, and so on.
System	Ticketing Log Feedback Log Connection Error System Connection Authentication failure Boot FTP Audit Low Battery on Remote Control	Catches errors and other events from systems.
Network	Packet Loss Log Packet Loss Conference Bandwidth Usage Network History	Statistics reports on network and bandwidth usage.
Return on Investment	Return on Investment Global Return on Investment Local	Return on Investment and C02 Savings calculate return on investment and environmental savings for your video equipment.
C02 Savings		Return on Investment and C02 Savings calculate return on investment and environmental savings for your video equipment.
Reporting Template		Any search can be stored and reused as a template.

Summary

This chapter focused on how TMS can be used to streamline and simplify the daily tasks of using and managing a Cisco collaboration network all from a single, easy-to-use web interface. Although this lesson did not give an exhaustive explanation of all the tasks TMS is able to perform, it did outline the main functions for which TMS is most commonly used. This lesson introduced how to add systems to be managed by TMS, how to view open tickets on those systems, and how to schedule and manage conferences from TMS and overviewed some of the reporting tools available on TMS.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 16-4 lists a reference of these key topics and the page numbers on which each is found.

Table 16-4 Key Topics for Chapter 16

Key Topic Element	Description	Page Number
Table 16-2	Know the protocols and ports TMS uses to communicate across a network.	354
Paragraph	Understand the purpose of TMSPE and TMSXE.	355
Paragraph	Know the mechanism TMS uses to manage systems.	356
Paragraph	Know the two operations an administrator can perform on tickets TMS generates.	359
Bulleted List	Know the different types of conferences that TMS can create.	360
Paragraph	Understand how to use the Smart Scheduler option within TMS.	363
Paragraph	Know that Java is an important component in TMS used to access the Conference Control Center.	364
Table 16-3	Know the different reporting options in TMS and their purpose.	366

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

TMS, SQL, IIS, .NET, TMSPE, TMSXE, SNMP, TCS, Smart Scheduler, ROI, CDR

This chapter covers the following topics:

- **WebEx Products and Features:** This section introduces the concept of WebEx as a cloud-based collaboration meeting space and overviews the different products available within the Cisco WebEx solution.
- **WebEx Meeting Center:** This section examines the features available with Cisco's pinnacle product, WebEx Meeting Center.

Cisco WebEx Solutions

With the ever-changing workplace, keeping up with business needs and trends can often be a strenuous task. Add in the complexity and frequency with which newer technologies are entering the market, and it becomes increasingly obvious why businesses that cannot keep up with these trends fail. In an effort to stay in front of these workplace transformations, Cisco seeks out key acquisitions that keep them at the top of the market as number one or two in any commerce of which they are a part.

One key acquisition Cisco made in 2007 was a company known as WebEx. With keen foresight about the direction the industry was heading, WebEx has placed Cisco strongly in the number-one position for cloud-based collaboration meeting space solutions. Cisco has continued to develop the service offering available with WebEx, recently launching the Collaboration Meeting Rooms (CMR) solution. This chapter introduces the different WebEx solutions available in the market today and reviews some of the features and tools that enhance the collaboration experience.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 17-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already? Quizzes."

Table 17-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
WebEx Products and Features	1–3
WebEx Meeting Center	4–8

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which Cisco WebEx solution offers breakout sessions?

   a. Cisco WebEx Meeting Center
   b. Cisco WebEx Support Center
   c. Cisco WebEx Training Center
   d. Cisco WebEx Event Center

2. Which of the following is a feature of Cisco WebEx IM?

   a. Emoticons
   b. Attentiveness tool
   c. Follow-up tool
   d. Content sharing

3. Which of the following Cisco WebEx solutions is available as an on-premises or cloud solution?

   a. Cisco WebEx Meeting Center
   b. Cisco WebEx Support Center
   c. Cisco WebEx Training Center
   d. Cisco WebEx Event Center

4. What port does Cisco WebEx Meeting Center use for clients to connect to a meeting?

   a. 5060
   b. 5061
   c. 1720
   d. 443

5. What is the maximum number of client participants that can join a Cisco WebEx Meeting Center session?

   a. 500
   b. 5000
   c. 300
   d. 3000

6. Which of the following is not a function of Cisco WebEx Meeting Center?

   a. File transfer
   b. Share a file or application
   c. Whiteboard
   d. Emoticons

7. How many video endpoints can join a meeting using CMR Cloud?

   a. 1
   b. 25
   c. 100
   d. 1000

8. How many video endpoints can join a meeting using CMR Hybrid?

   a. 1
   b. 25
   c. 100
   d. 1000

Foundation Topics

WebEx Products and Features

Cisco has established themselves as the global leader in many venues, including on-demand applications for collaborative business in the cloud through the Cisco WebEx product line. Using Cisco WebEx collaboration products, you can conduct online meetings over the Web in real time, from anywhere, anytime, and on any device. The WebEx solution is a web-based software-as-a-service (SaaS) conferencing solution that supports 720p30 HD video using the H.264 codec. Any PC or mobile devices with a camera, microphone, speakers, and Internet connectivity can join meetings. The audio connection can be deployed either over IP through the web client device or with a dedicated phone using the callback or dial-in feature across the public switched telephone network (PSTN).

Ad hoc conferences can be initialized with a Cisco WebEx productivity tool using Cisco WebEx One-Click features. Cisco WebEx One-Click enables you to start a meeting and invite attendees instantly from your desktop, taskbar, or favorite applications. The ad hoc meeting information can be pushed to other participants through e-mail and instant messaging (IM). Conferences can be scheduled regularly through the groupware client using Cisco WebEx productivity tools and e-mail client plug-ins. Integration is available with Microsoft Exchange and Lotus Notes. Cisco WebEx is not a one-size-fits-all single solution, although the main Cisco product can fit most business needs. Cisco WebEx includes several products that cater to differing business requirements. Table 17-2 outlines the different WebEx products available and some of the key features each solution offers.

Key Topic

Table 17-2 Cisco WebEx Products and Features

Cisco WebEx Product	Cisco WebEx Feature
WebEx Meeting Center	Audio, HD video at 720p30, content sharing, file transfer, polling, remote desktop control
WebEx Connect IM	A client-based application running on a PC that offers audio, HD video at 720p30, content sharing, and instant messaging through the WebEx cloud
WebEx Training Center	All the features of WebEx Meeting Center plus breakout sessions, emoticons, and an attentiveness tool
WebEx Event Center	All the features of WebEx Meeting Center plus a scheduling and follow-up tool and support for up to 3000 participants
WebEx Support Center	Full technical support with a quicker fault-resolution time using all the features of WebEx Meeting Center

Cisco WebEx Meeting Center is the pinnacle solution that combines file and presentation sharing with voice, high-definition video, and new meeting spaces. Cisco WebEx Meeting Center is available as a cloud service, which means that there is no need to purchase and support a bunch of endpoints and servers. This allows small and medium-sized businesses to leverage voice and video communications technology without a large initial investment.

WebEx Meeting Center can also be offered as an on-premises solution. The on-premises solution can be customized with the organization's logo, and features are more easily managed. Cisco CMR Cloud and Cisco CMR Hybrid leverage WebEx Meeting Center Cloud to connect WebEx users and traditional TelePresence endpoints together in a single collaboration environment, while preserving the end-user experience.

Cisco WebEx Connect IM brings together presence, enterprise IM, audio, video, web conferencing, and IP telephony through one client. Cisco WebEx Connect IM is similar to Microsoft Lync or Cisco Jabber. A client can be downloaded to a computer and communicates with the WebEx cloud. There is no upfront investment, and no maintenance or upgrade costs, just a predictable monthly subscription. So, it is easy to implement and easy to scale as business needs change.

Cisco WebEx Training Center offers all the same features as WebEx Meeting Center, with a few more options needed in a virtual classroom environment. Cisco WebEx Training Center delivers highly interactive classes and training online, with video, breakout sessions, and hands-on learning labs. This application of WebEx can be used to train employees or offer online courses. Scheduling tools allow administrators to schedule a series of sessions, offer open attendance, or require registration. Emoticons allow participants to interact with the presenter and each other. A coffee cup can be displayed to show you are on a break, a hand can be raised if you have questions, and other icons can be used at the presenter's discretion to demonstrate participation. An attentiveness tool is built in that shows whether participants are on the WebEx page or if they are viewing something else on their computer. These are just a few of the options available with the Cisco WebEx Training Center solution.

Cisco WebEx Event Center provides the tools that you need to deliver cost-effective and successful online events. These events could range from event planning and promotion, to delivery and post-event follow-up and campaign reporting. Cisco WebEx Event Center enables companies to host events with up to 3000 participants and to control every aspect of the event from who is invited to following up with participants after the event. Cisco WebEx Event Center can be used to qualify, track, and cultivate leads for your sales initiatives, and can capture attendee information that can be stored and accessed later.

Cisco WebEx Support Center provides real-time IT support and customer service to employees and customers anywhere in the world. The Cisco WebEx Collaboration Cloud, which is a real-time global network that provides fast, reliable, and secure application delivery, provides all Cisco WebEx cloud services.

WebEx Meeting Center

Because all WebEx products are based on the Cisco WebEx Meeting Center platform, this product warrants a more detailed description of the features offered. This chapter has already established that Cisco WebEx Meeting Center allows participants to present information, share applications, and collaborate on projects. It streamlines the meeting process with a centralized space for managing activities and information. Cisco WebEx Meeting Center can be used for collaborative sessions, internal and external meetings, product and project coordination demos, and sales presentations. Table 17-3 outlines the Cisco WebEx Meeting Center features that are discussed in this section.

Key Topic

Table 17-3 Cisco WebEx Meeting Center Features with Descriptions

Feature	Description
TCP communication	Uses port 80 over HTTP and port 443 over HTTPS.
HD video	Uses the H.264 video codec for high-quality 720p30 HD video at low bandwidth rates.
Content sharing	Anyone in the meeting who holds the "WebEx ball" can share a file, share an application, or share your desktop through WebEx.
Remote desktop control	Once participants shares their desktop, another participant can take control of the desktop in a secure fashion after permissions have been granted.
Participant capacity	Up to 500 participants can join a fully licensed WebEx Meeting Center session.
Recording	Meetings can be recorded over WebEx. After the meeting has ended, the recording can be streamed for playback or downloaded and played back on-demand.
File transfer	Files and applications can be transferred to all participants within a WebEx session for download.

Cisco WebEx Meeting Center can be deployed using TCP port 80 over HTTP or port 443 over HTTPS. This allows users to securely access WebEx meetings without having to deploy advanced security options within their network or open ports across their firewall. The domains that use these ports include WebEx.com and WebExConnect.com, as well as any subdomains, such as Company.WebEx.com. Table 17-4 provides a more complete list of ports WebEx uses.

Table 17-4 Ports Used by Cisco WebEx

Protocol	Port Number	Access Type
TCP	80	Client access
TCP	443	Client access – secure traffic (Secure Sockets Layer [SSL] sites)
TCP/UDP	1270	Client access (non-SSL sites)
TCP/UDP	53	Domain Name Server (DNS)
TCP/UDP	5101	Multichassis multilink PPP (MMP)
TCP	8554	Audio streaming client access
UDP	7500	Audio streaming
UDP	7501	Audio streaming

Protocol	Port Number	Access Type
UDP	9000	VoIP/video
UDP	9001	VoIP/video
TCP/UDP	5060-5069	SIP for CMR Hybrid and Cloud
UDP	30000-65535	Media for CMR Hybrid and Cloud
TCP	1720	H.323 for CMR Cloud
UDP	1719	H.323 for CMR Cloud
TCP	15000-19999	H.323 for CMR Cloud

WebEx uses the H.264 codec for multipoint high-quality video at 720p30. H.264 uses special compression algorithms that allow participants to stream HD video at low bandwidth rates of less than 1 Mbps. The Cisco WebEx full-screen video experience includes active speaker switching. The Cisco WebEx user interface has been modified to have a high-quality video experience in all screen views. It is easy to use and automatically adjusts video quality for each participant according to the participant's network bandwidth because different users can send and receive different resolutions. With the high-quality video capabilities and the TCP streaming capabilities, Cisco WebEx Meeting Center is a secure application that can operate with high-quality video for any company from any location in the world.

With Cisco WebEx Meeting Center, there are different ways to share content between participants, and content can be shared from any participant within the WebEx Meeting. The host of the meeting will have the Cisco WebEx ball icon displayed beside his or her name. Using the mouse to scroll over another participant's name will reveal a Cisco WebEx ball that is grayed out. To "pass the ball" to another participant, simply click the grayed-out ball beside that participant's name. That participant then takes control of the meeting and now has the ability to share content. You can also click the grayed-out ball beside your own name to "take the ball." If another participant is sharing content while the ball is passed, the content that is being shared will immediately drop from the session. Whoever is sharing content can choose to share a document, application, or their entire desktop. If a participant is sharing his desktop, another participant can request remote desktop control. A pop-up will display on the screen of the presenter, who must grant permission before another participant can take control. Resuming control of your own desktop is as simple as moving your mouse. After you have resumed control, the whole process must be repeated to grant someone else control again. Figure 17-1 illustrates content that is being shared over a WebEx Meeting Center session.

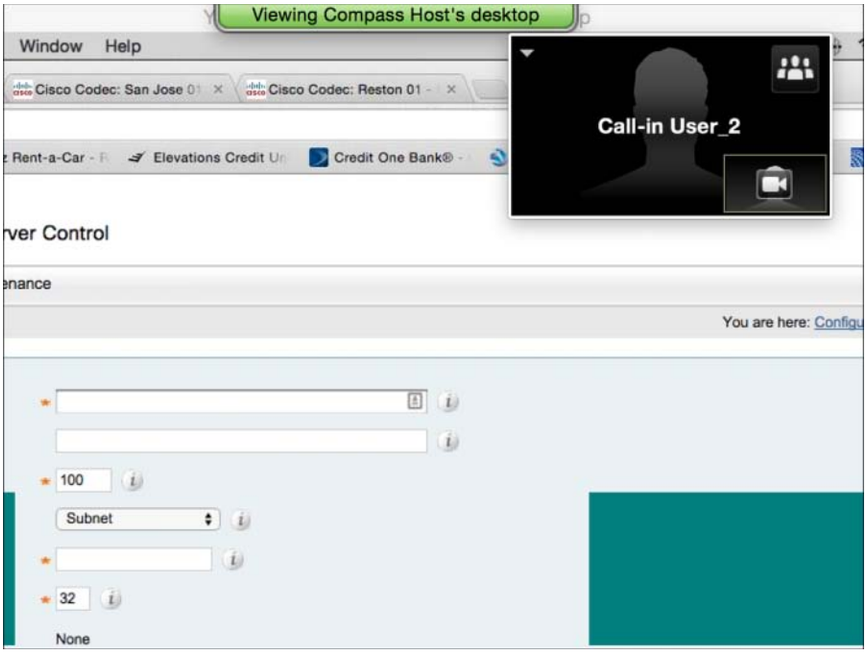


Figure 17-1 *Content Sharing over WebEx Meeting Center*

Sharing content through WebEx is a great way to express ideas and engage other participant in the conversation. Sometimes, however, premeditated content is not enough. Therefore, Cisco also offers an integrated Whiteboard feature and annotation tools with each WebEx session. With the Whiteboard feature, a presenter can add text blocks and draw shapes, lines, or even draw free style. Different colors can be used to make objects and lines more pronounced. All participants within a meeting, to make a selection within a Whiteboard drawing, can also use name arrows. These same annotation tools used with the Whiteboard feature can be used within content being shared, for similar purposes. Examples of how these annotation tools can be used include circling or underlining a word, phrase, or graphic to draw participants' attention to the topic being discussed. If a map is being shared, the name arrow can be used to show a participant's location or an area that a sales rep is targeting. On a graphic showing sales projection for the next quarter, the annotation tools could be used to draw lines of where projections should be or to highlight key elements that will impact these projections. However these tools are used, Cisco WebEx Meeting Center makes communication across distances a whole lot better by engaging participants and emphasizing key topics in a presentation. Figure 17-2 illustrates some of the options that you can use with the Whiteboard feature on Cisco WebEx Meeting Center.

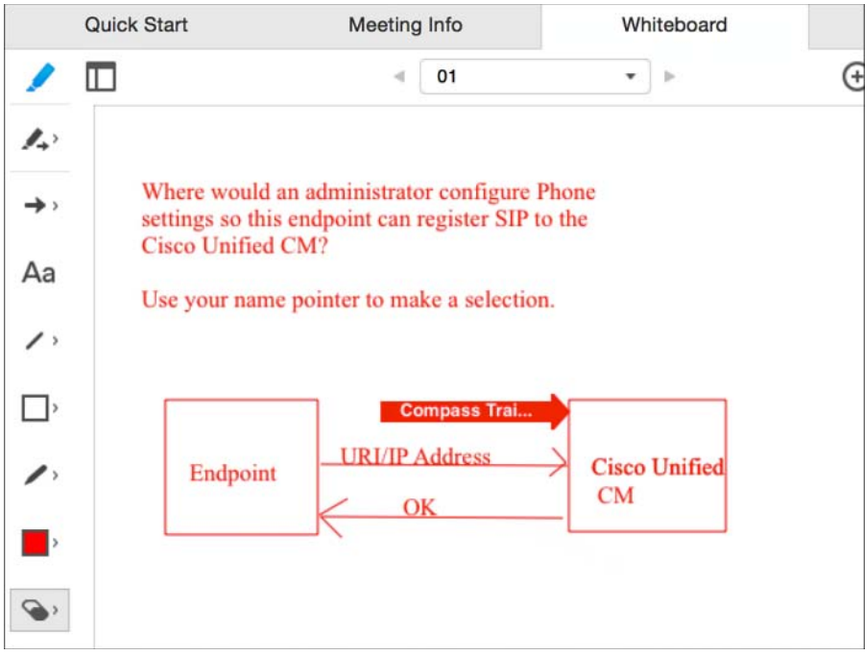


Figure 17-2 *Cisco WebEx Meeting Center Whiteboard Feature*

You do not have to use Cisco WebEx Event Center to support a large number of participants. Cisco WebEx Meeting Center can scale from one to hundreds of attendees. The host can then control what privileges each participant has within the meeting. The host may only want the participants to see and hear the information being shared, without offering any kind of interaction. Such an application may be a CEO making a state of the company address to an entire body of employees. If a presentation is being made and questions about the content are anticipated but time is of the essence, a chat-only feature can be allowed for the majority of participants and a smaller team of panelists can be used to answer questions as they are asked, while the main host continues with the presentation.

Another great feature offered with Cisco WebEx Meeting Center is the ability to record meetings. With WebEx Premises, recorded meetings are stored on your local server. With Cisco WebEx Meeting Center Cloud, recorded meetings are stored in the cloud. Participants can then be invited to review recorded meetings or optionally download them for reference later. WebEx does have a storage fee for recordings, but because they can be downloaded, hosts can download and delete recorded meetings and then host access to the recorded meetings from their own on-premises streaming server. Cisco TelePresence Content Server (CTS) or Cisco Show and Share (SnS) are two great applications for streaming content. The Cisco Media Experience Engine (MXE) can be used to change the format and add analytics to the WebEx recorded content. Figure 17-3 illustrates the recording option available with Cisco WebEx Meeting Center.

Figure 17-3 *Cisco WebEx Meeting Center Recording Feature*

In addition to all these other features available within a Cisco WebEx Meeting Center session, files and applications can be transferred to all participants within a WebEx session for download. The host simply has to enable the option to transfer a file. A pop-up window will appear with two options: **Share File** and **Download**. The host needs to click the **Share File** button and select the files or applications he wants to share. These selections appear in the same pop-up window on all participants' computers. Then, if they just click one of the items in the list and then click the **Download** button, the item will download from WebEx to their personal computer. Figure 17-4 illustrates the pop-up window that can be used in WebEx Meeting Center to transfer files and applications.

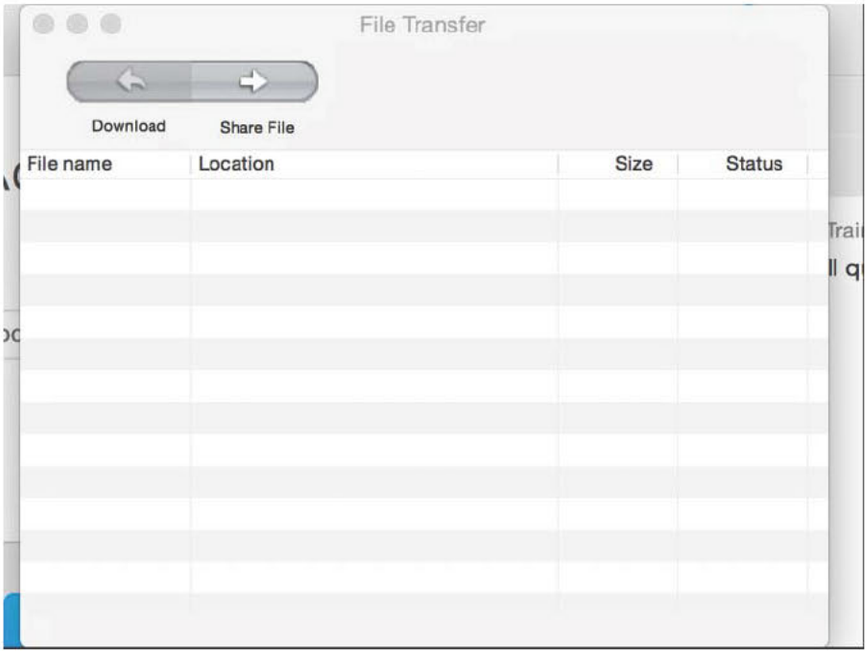


Figure 17-4 *WebEx Meeting Center File Transfer Feature*

Key Topic

In addition to all the tools available within Cisco WebEx Meeting Center, it can also be used as the conference-bridging source for WebEx clients and physical endpoints within a collaboration solution. This function of Cisco WebEx Meeting Center is known as Cisco CMR Cloud. Cisco CMR Cloud is a quickly enabled, maintenance-free service that can scale based on your customer's needs. Offered as an add-on service option to a Cisco WebEx Meeting Center subscription, Cisco CMR Cloud is delivered exclusively through the Cisco WebEx Cloud. Similar to CMR Hybrid, anyone with a standards-based endpoint or web client can join a meeting. Up to 25 participants with standards-based video endpoints and up to 500 video-enabled WebEx Meeting Center users can join the same meeting.

Key Topic

CMR Hybrid enables customers to extend the reach and scale of meetings by augmenting their CMR Premises deployment with a subscription to Cisco WebEx Meeting Center. It enables customers to quickly extend their on-premises Cisco collaboration services to include Cisco WebEx Meeting Center users wherever they may be, either inside or outside the enterprise, or even mobile. Anyone can join a meeting from Cisco video endpoints, third-party standards-based video endpoints and UC clients, and from soft clients such as Cisco Jabber or Cisco WebEx-enabled mobile or desktop web clients. Participants with standards-based video endpoints are limited in number of participants by the on-premises infrastructure, and up to 500 video-enabled WebEx Meeting Center users can join a single meeting. If customers have already fully licensed both WebEx and video infrastructure, they can add CMR Hybrid functionality to their deployments for no additional cost.

CMR Hybrid, formerly known as Cisco TelePresence WebEx OneTouch 2.0, extends Cisco TelePresence meetings to Cisco WebEx users. It blends the ease of use and broad reach of both Cisco TelePresence and Cisco WebEx solutions into one collaborative solution. It enables two-way video, audio, and content sharing between attendees using any type of TelePresence endpoints and WebEx conference participants, including mobile users. With Cisco TelePresence WebEx OneTouch, a meeting host can launch a joint Cisco TelePresence and WebEx meeting with the simplicity of One Button to Push (OBTP). To schedule a meeting, an organizer can use a Microsoft Outlook integration that the WebEx Productivity Tools enable. The host selects the participants, adds the preferred TelePresence endpoint and the WebEx information, and sends the invitation to all participants. CMR Hybrid displays the participant list in the Cisco WebEx meeting client and in the welcome screen for the Cisco TelePresence attendees. Cisco Unified Communications Manager or Cisco TelePresence Video Communication Server (Cisco VCS) for Cisco TelePresence endpoints enables CMR Hybrid. Cisco VCS Expressway is required for connectivity to WebEx meetings through a corporate firewall. Supported Cisco TelePresence multipoint conferencing systems include Cisco TelePresence Server and Cisco TelePresence MCU. Scheduling of the CMR Hybrid conferences requires Cisco TelePresence Management Suite (Cisco TMS).

Summary

Cisco has established themselves as the global leader in many venues, including on-demand applications for collaborative business in the cloud through the Cisco WebEx product line. Using Cisco WebEx collaboration products, you can conduct online meetings over the web in real time, from anywhere, anytime, and on any device. Any PC or mobile devices with a camera, microphone, speakers, and Internet connectivity can join meetings. Cisco WebEx includes several products that cater to differing business requirements. These products include the pinnacle product, Cisco WebEx Meeting Center. In addition to this product, there are Cisco WebEx Training Center, Cisco WebEx Connect IM, Cisco WebEx Event Center, and Cisco WebEx Support Center.

Cisco WebEx Meeting Center allows participants to present information, share applications, and collaborate on projects. It streamlines the meeting process with a centralized space for managing activities and information. Cisco WebEx Meeting Center can be used for collaborative sessions, internal and external meetings, product and project coordination demos, and sales presentations. Many tools available within a WebEx meeting enhance the presentation and convalesces abettor participation. Cisco CMR Cloud allows up to 25 participants with a standards-based endpoint, and up to 500 participants with the web client, to join a meeting. Cisco CMR Hybrid leverages both Cisco WebEx Meeting Center and on-premises video infrastructure to allows up to 100 participants with a standards-based endpoint, and up to 500 participants with the web client, to join a meeting. With Cisco TelePresence WebEx OneTouch, a meeting host can launch a joint Cisco TelePresence and WebEx meeting with the simplicity of OBTP.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 18, "Final Preparation," and the exam simulation questions on the CD.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 17-5 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 17-5 Key Topics for Chapter 17

Key Topic Element	Description	Page Number
Table 17-2	Know the different WebEx solutions available and the key features that differentiate between them.	374
Table 17-3	Know the different Cisco WebEx Meeting Center features available.	376
Paragraph	Understand what CMR Cloud offers in contrast to WebEx as an independent platform and the number of participants who can join a CMR Cloud session.	381
Paragraph	Understand what components make up CMR Hybrid and the number of participants who can join a CMR Hybrid session.	381

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Table Answer Key," also on the CD, includes completed tables and lists so that you can check your work.

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

SaaS, H.264, HD, PSTN, WebEx One-Click, CMR, CMR Cloud, CMR Hybrid, TCP, HTTP, HTTPS, OBTP, IM

The first 17 chapters of this book cover the technologies, protocols, commands, and features required to be prepared to pass the 210-065 CIVND (Implementing Cisco Video Network Devices) exam to become certified as a CCNA Collaboration professional. Although these chapters supply the detailed information, most people need more preparation than just reading alone. This chapter details a set of tools and a study plan to help you complete your preparation for the exam.

This short chapter has two main sections. The first section explains how to install the exam engine and practice exams from the CD that accompanies this book. The second section lists some suggestions for a study plan, now that you have completed all the earlier chapters in this book.

Note Appendixes C, D, and E exist as soft-copy appendixes on the CD included in the back of this book.

Final Preparation

Tools for Final Preparation

This section lists some information about exam preparation tools and how to access the tools.

Exam Engine and Questions on the CD

The CD in the back of the book includes the Pearson Cert Practice Test engine. This software presents you with a set of multiple-choice questions, covering the topics you will be likely find on the real exam. The Pearson Cert Practice Test engine lets you study the exam content (using study mode) or take a simulated exam (in practice exam mode).

The CD in the back of the book contains the exam engine. Once installed, you can then activate and download the current CIVND exam from Pearson's website. Installation of the exam engine takes place in two steps:

Step 1. Install the exam engine from the CD.

Step 2. Activate and download the CICD practice exam.

Install the Exam Engine

The following are the steps you should perform to install the software:

Step 1. Insert the CD into your computer.

Step 2. The software that automatically runs is the Cisco Press software to access and use all CD-based features, including the exam engine and the CD-only appendixes. From the main menu, click the option to **Install the Exam Engine**.

Step 3. Respond to the prompt windows as you would with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the CD sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam. Therefore, please register when prompted. If you already have a Pearson website login, there is no need to register again; just use your existing login.

Activate and Download the Practice Exam

Once the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process) as follows:

Step 1. Start the Pearson Cert Practice Test (PCPT) software.

Step 2. To activate and download the exam associated with this book, from the **My Products** or **Tools** tab, click the **Activate** button.

Step 3. At the next screen, enter the activation key from the paper inside the cardboard CD holder in the back of the book. Once entered, click the **Activate** button.

Step 4. The activation process downloads the practice exam. Click **Next**; then click **Finish**.

Once the activation process is completed, the **My Products** tab should list your new exam. If you do not see the exam, make sure you selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam, and click the **Use** button.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab, and select the **Update Products** button. Updating your exams will ensure you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, simply select the **Tools** tab, and click the **Update Application** button. This will ensure you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process, and the registration process, only has to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another new Cisco Press Official Cert Guide or Pearson IT Certification Cert Guide, remove the activation code from the CD sleeve in the back of that book; you do not even need the CD at this point. From there, all you have to do is start the exam engine (if not still up and running), and perform Steps 2 through 4 from the previous list.

Premium Edition

In addition to the free practice exam provided on the CD-ROM, you can purchase additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition of this title contains an additional two full practice exams and an eBook (in both PDF and ePub format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

Because you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. A coupon in the CD sleeve contains a one-time-use code and instructions for where you can purchase the Premium Edition.

To view the premium edition product page, go to www.ciscopress.com/title/9781587144424.

The Cisco Learning Network

Cisco provides a wide variety of CCNA Collaboration preparation tools at a Cisco website called the Cisco Learning Network. Resources found here include sample questions, forums on each Cisco exam, learning video games, and information about each exam.

To reach the Cisco Learning Network, go to http://learningnetwork.cisco.com, or just search for "Cisco Learning Network." To access some of the features/resources, you need to use the login you created at Cisco.com. If you do not have such a login, you can register for free. To register, simply go to Cisco.com, click **Register** at the top of the page, and supply some information.

Memory Tables

Like most Certification Guides from Cisco Press, this book purposefully organizes information into tables and lists for easier study and review. Rereading these tables can be very useful before the exam. However, it is easy to skim over the tables without paying attention to every detail, especially when you remember having seen the table's contents when reading the chapter.

Instead of simply reading the tables in the various chapters, this book's Appendixes C and D give you another review tool. Appendix C, "Memory Tables," lists partially completed versions of many of the tables from the book. You can open Appendix C (a PDF on the CD that comes with this book) and print the appendix. For review, you can attempt to complete the tables. This exercise can help you focus during your review. It also exercises the memory connectors in your brain; plus it makes you think about the information without as much information, which forces a little more contemplation about the facts.

Appendix D, "Memory Table Answer Key," also a PDF located on the CD, contains the completed tables to check yourself. You can also just refer to the tables as printed in the book.

Chapter-Ending Review Tools

Chapters 1 through 17 each have several features in the "Exam Preparation Tasks" section at the end of the chapter. You may have used some of or all these tools at the end of each chapter. It can also be useful to use these tools again as you make your final preparations for the exam.

Study Plan

With plenty of resources at your disposal, you should approach studying for the CCNA Collaboration exam with a plan. Consider the following ideas as you move from reading this book to preparing for the exam.

Recall the Facts

As with most exams, many facts, concepts, and definitions must be recalled to do well on the test. If you do not work with security technologies and features on a daily basis, you might have trouble remembering everything that might appear on the CCNA Collaboration exam.

You can refresh your memory and practice recalling information by reviewing the activities in the "Exam Preparation Tasks" section at the end of each chapter. These sections will help you study key topics, memorize the definitions of important security terms, and recall the basic command syntax of configuration and verification commands.

Practice Configurations

The CCNA Collaboration exam includes an emphasis on practical knowledge. You need to be familiar with switch features and the order in which configuration steps should be implemented.

This means that hands-on experience is going to take you over the edge to confidently and accurately build or verify configurations (and pass the exam). If at all possible, you should try to gain access to some endpoints, such as 8945 or 9971 IP Video Phones, Jabber Client and Jabber Video for TelePresence soft clients, CTS 500, DX series endpoint, and any of the TC software-based endpoints. For registering and placing calls, you need access to the Cisco Unified Communications Manager (CM), Cisco IM and Presence Service, and Cisco Video Communication Server (VCS). For multipoint calls, you need access to a Cisco TelePresence MCU and a Cisco TelePresence Management Suite (TMS). I know that is a tall order, but we cannot avoid the fact that hands-on experience means you need to get your hands on some gear.

If you have access to a lab provided by your company, take advantage of it. You might also have some Cisco equipment in a personal lab at home. Otherwise, there are a number of sources for lab access, including online rack rentals from trusted Cisco Partners and the Cisco Partner E-Learning Connection (PEC), if you work for a Partner. Nothing beats hands-on experience.

In addition, you can review the key topics in each chapter and follow the example configurations in this book. At the least, you will see the command syntax and the sequence in which configuration commands should be entered.

Using the Exam Engine

The Pearson Cert Practice Test engine on the CD lets you access a database of questions created specifically for this book. The Pearson Cert Practice Test engine can be used either in study mode or practice exam mode, as follows:

- **Study mode:** Study mode is most useful when you want to use the questions for learning and practicing. In study mode, you can select options like randomizing the order of the questions and answers, automatically viewing answers to the questions as you go, testing on specific topics, and many other options.

- **Practice Exam mode:** This mode presents questions in a timed environment, providing you with a more exam realistic experience. It also restricts your ability to see your score as you progress through the exam and view answers to questions as you are taking the exam. These timed exams not only allow you to study for the actual 210-065 CIVND exam, they also help you simulate the time pressure that can occur on the actual exam.

When doing your final preparation, you can use study mode, practice exam mode, or both. However, after you have seen each question a couple of times, you will likely start to remember the questions, and the usefulness of the exam database may go down. So, consider the following options when using the exam engine:

- Use the question database for review. Use study mode to study the questions by chapter, just as with the other final review steps listed in this chapter. Consider upgrading to the Premium Edition of this book if you want to take additional simulated exams.
- Save the question database, not using it for review during your review of each book part. Save it until the end so that you will not have seen the questions before. Then, use practice exam mode to simulate the exam.

To select the exam engine mode, click the **My Products** tab. Select the exam you want to use from the list of available exams, and then click the **Use** button. The engine should display a window from which you can choose **Study Mode** or **Practice Exam Mode**. When in study mode, you can further choose the book chapters, limiting the questions to those explained in the specified chapters of the book.

APPENDIX A

Answers to the "Do I Know This Already?" Quizzes

Chapter 1

1. B
2. C
3. A
4. B
5. D

Chapter 2

1. B
2. A
3. B
4. B
5. A
6. C
7. B
8. D

Chapter 3

1. B
2. D
3. B
4. A
5. C
6. D
7. B
8. C
9. B

Chapter 4

1. B
2. A
3. A
4. A, B, C
5. C
6. B
7. B
8. A, B
9. A

Chapter 5

1. C
2. D
3. C
4. C
5. A
6. A
7. D
8. B
9. A
10. C

Chapter 6

1. A, D
2. C, D
3. C
4. A
5. B

6. A
7. C
8. B
9. C, D
10. C
11. A
12. B
13. D
14. C
15. A
16. D
17. A
18. A
19. C
20. B

Chapter 7

1. B
2. D
3. B
4. B
5. D
6. D
7. B
8. C
9. B
10. C

Chapter 8

1. A
2. C
3. D
4. B
5. B
6. C
7. A
8. C
9. A
10. D

Chapter 9

1. C
2. B
3. D
4. C
5. A
6. A
7. C
8. A
9. B
10. D

Chapter 10

1. B
2. C
3. D
4. B
5. B
6. C
7. A
8. C
9. A
10. C

Chapter 11

1. D
2. A
3. B
4. D
5. D
6. B

7. B
8. A
9. C
10. A

Chapter 12

1. B
2. A
3. D
4. A
5. C
6. C
7. B
8. C
9. A
10. D

Chapter 13

1. B
2. A
3. B
4. C
5. D
6. A
7. C
8. D
9. B
10. D

Chapter 14

1. D
2. A
3. B
4. B
5. A
6. D
7. C
8. C
9. A
10. C

Chapter 15

1. B
2. C
3. D
4. A
5. C
6. A
7. C

Chapter 16

1. C
2. D
3. B
4. A
5. C
6. A
7. B
8. C
9. D
10. A

Chapter 17

1. C
2. D
3. A
4. D
5. A
6. D
7. B
8. C

CCNA Collaboration 210-065 (CIVND) Exam Updates

Over time, reader feedback allows Cisco Press to gauge which topics give our readers the most problems when taking the exams. To assist readers with those topics, the authors create new materials clarifying and expanding upon those troublesome exam topics. As mentioned in the introduction, the additional content about the exam is contained in a PDF document on this book's companion website, at http://www.ciscopress.com/title/9781587144424.

This appendix is intended to provide you with updated information if Cisco makes minor modifications to the exam upon which this book is based. When Cisco releases an entirely new exam, the changes are usually too extensive to provide in a simple update appendix. In those cases, you might need to consult the new edition of the book for the updated content.

This appendix attempts to fill the void that occurs with any print book. In particular, this appendix does the following:

Mentions technical items that might not have been mentioned elsewhere in the book

Covers new topics if Cisco adds new content to the exam over time

Provides a way to get up-to-the-minute current information about content for the exam

Always Get the Latest at the Companion Website

You are reading the version of this appendix that was available when your book was printed. However, given that the main purpose of this appendix is to be a living, changing document, it is important that you look for the latest version online at the book's companion website. To do so:

Step 1. Browse to http://www.ciscopress.com/title/9781587144424.

Step 2. Select the Appendix option under the More Information box.

Step 3. Download the latest "Appendix B" document.

Note Note that the downloaded document has a version number. Comparing the version of the print Appendix B (Version 1.0) with the latest online version of this appendix, you should do the following:

Same version: Ignore the PDF that you downloaded from the companion website.

Website has a later version: Ignore this Appendix B in your book, and read only the latest version that you downloaded from the companion website.

Technical Content

The current version of this appendix does not contain any additional technical coverage.

Glossary

.NET The Microsoft programming framework on which Internet Information Services (IIS) is built and operates.

2B+D A designation for an ISDN BRI implementation including two bearer channels and one data channel.

23B+D A designation for an ISDN PRI (T1) implementation including 23 bearer channels and 1 data channel.

30B+D A designation for an ISDN PRI (E1) implementation including 30 bearer channels and 1 data channel.

720p30 An abbreviation for video transmission at 720p resolution at 30 frames per second.

720p60 An abbreviation for video transmission at 720p resolution at 60 frames per second.

802.11a/b/g/n/ac Standards for wireless local-area network radio transmission and associated data rates. Typically, devices with wireless network adapters will be listed as 802.11 capable followed by a list of the radios supported. In this case, 802.11a/b/g/n/ac denotes support for 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac standards.

802.3af PoE A standard for providing a maximum of 15.4 watts of DC power to a PoE-capable device. The 802.3af standard defines only the use of Classes 0, 1, 2, and 3. Class 4 devices require 802.3at.

802.3at PoE A standard for providing a maximum of 25.5 watts of DC power to a PoE-capable device. Class 4 devices must have 802.3at power available to function. This is also known as PoE+.

1080p30 An abbreviation for video transmission at 1080p resolution at 30 frames per second.

ACF Admission confirm; part of the H.323 RAS messaging. Sent from the gatekeeper to an endpoint confirming call setup can proceed.

Active Load The currently installed and running firmware version on a Cisco IP Phone.

AD Active Directory (AD) is a Microsoft LDAP product that stores and shares information in environments that require high-availability access to user account information.

Ad hoc Not scheduled. Cisco defines an ad hoc conference as any conference where the participants joining the conference are not scheduled.

AGC Automatic gain control is used with audio equipment to help equalize the sound transmitting through speakers and microphones to help reduce the amount of echo and feedback heard.

Allow Control of Device from CTI The CTI control service on the Cisco Unified CM allows a phone to be controlled by the Jabber soft client, meaning when Jabber sends or receives a call request, the media and signaling is rerouted through the associated phone.

Analog terminal adapter (ATA) An IP telephony endpoint that enables the connection of analog-based stations, such as phones and fax machines, to the IP network.

API Application programming interface. The code-line interface used by programmers and equipment administrators to issue advanced-level commands to the system.

ARJ Admission reject; part of the H.323 RAS messaging. Sent from the gatekeeper to an endpoint confirming the call attempt failed.

ARQ Admission request; part of the H.323 RAS messaging. Sent from an endpoint to the gatekeeper to request a call be established.

Artifact-removal technology Cisco provides computationally advanced filters to remove visual artifacts left by poor endpoints or low-bandwidth encoders (such as 3G devices) to provide improved images.

Assent Cisco proprietary protocol that allows NAT and firewall traversal in a secure environment with use of only a few ports.

Auto attendant A virtual receptionist feature available on MCUs. Auto attendants are used as a means for participants to choose what conference they want to join. Auto participants will hear an interactive voice response (IVR), which auto attendants are often referred to as.

Auto-registration A capability in CUCM that allows for phones to be connected to the network, register, and receive a directory number without any phone-specific administrative configuration.

Basic Rate Interface (BRI) BRI is an ISDN interface to basic rate access. Basic rate access consists of a single 16-kbps D channel plus two 64-kbps B channels for voice or data.

Binary Floor Control Protocol (BFCP) Binary Floor Control Protocol is a protocol for controlling access to the media resources in a conference. It is also used in embedding shared content into a video stream during a video call or videoconference.

BNC Bayonet Neill-Concelman connectors are used on coaxial cable. They could be used in composite or component video connections.

BRI Basic Rate Interface. BRI links have two B channels that support 64 kbps and one D channel that supports 16 kbps.

Bulk Administration Tool (BAT) A utility within CUCM that allows for mass modification of phones, users, directory numbers, gateways, and other devices.

Busy Lamp Field (BLF) A button defined on a phone for the express purpose of monitoring the line state of another phone.

Call Admission Control (CAC) Call admission control refers to one of several techniques for monitoring the total remaining bandwidth available for voice traffic over a WAN link. The purpose of CAC is to prevent the transmission of voice traffic in excess of what the link can support without overflowing the QoS voice priority queue and causing voice packets to be dropped by the router, resulting in very poor quality for all concurrent calls. CAC can be implemented using the CUCM locations configuration within or between clusters, using RSVP, or using gatekeeper routers.

Call control An central or distributed entity that provides signaling; destination route pattern lookup; connection admission control; class of restriction; and other operations associated with call setup, state change, and teardown in telephony or video infrastructure deployments.

Calling search space (CSS) Partitions can be seen as a collection of route patterns. Directory numbers, route patterns, and translation patterns can all belong to specific partitions. A CSS is an ordered list of route partitions, and a CSS determines which partitions calling devices must search when they attempt to complete a call.

CCTV Closed-circuit television is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.

CDP Cisco Discovery Protocol. Proprietary protocol used by Cisco devices to discover VLAN information from Cisco switches.

CDR Call detail record.

Chrominance Color levels and mixtures that are broken out when converting video to digital format.

Cisco Audio Session Tunnel (CAST) Allows IP Phones and associated applications behind the phone to discover and communicate with the remote endpoints without requiring changes to traditional signaling components.

Cisco CallManager CCMCIP A service that runs on Cisco Unified Communications Manager and retrieves a list of devices associated with each user.

Cisco Cast An subsystem component of the Cisco Digital Media Suite architecture that allows delivery of live and on-demand video, broadcast television, and other content to digital screens via Cisco digital media players.

Cisco Discovery Protocol (CDP) Cisco proprietary protocol created in 1994 to provide a mechanism for management systems to automatically learn about devices connected to the network. Endpoints use CDP to communicate with the LAN switch regarding the ID of the voice/video VLAN, per-port power management details, and QoS information.

Cisco IPICS The Cisco Physical Access Manager appliance is a physical intrusion-detection solution using Cisco Physical Access Gateway devices to connect conventional wired sensors, along with other physical-security elements through a converged IP network.

Cisco Prime Collaboration A suite of products and capabilities that automate network management, monitoring, and lifecycle to improve the voice and video collaborative experience

Cisco TelePresence Server (CTS) A scalable videoconferencing bridge that works with Cisco Unified Communications Manager to bring multiparty video to unified communications deployments.

Cisco Unified Communications Manager (CUCM) An IP-based collaboration call control platform developed and sold by Cisco Systems for the purpose of delivering the right user experience to the right endpoint by integrating voice, video, data, and mobility products and applications.

Cisco Unified Mobility A call mobility option on the Cisco Unified CM that allows multiple endpoints to ring when the alias of a singe endpoint is dialed.

Cisco Video Media Server Software Responsible for the recording, storing, and streaming of video feeds.

Cisco Video Operations Manager Software Offers centralized administration of all the Cisco video-surveillance solution components and supports Cisco video surveillance endpoints.

Cisco Video Virtual Matrix Software Supporting many layouts, operators can choose a predefined layout of cameras and push it out to the displays of all users or choose to send different users various layouts with differing camera feeds.

Cisco WebEx Meetings Server (CWMS) An on-premises instance of the WebEx Meeting Center platform. It offers a highly secure, fully virtualized, behind-the-firewall conferencing solution that combines audio, video, and web conferencing in a single solution.

Class 0 PoE Power over Ethernet classification providing 0.44–12.94 watts / 0–4 mA. Class 0 is currently referenced as unimplemented or reserved.

Class 1 PoE Power over Ethernet classification providing 0.44–3.84 watts / 9–12 mA. Class 1 devices are classified as Very Low Power devices.

Class 2 PoE Power over Ethernet classification providing 3.84–6.49 watts / 17–20 mA. Class 2 devices are classified as Low Power devices.

Class 3 PoE Power over Ethernet classification providing 6.49–12.95 watts / 26–30 mA. Class 3 devices are classified Mid Power devices.

Class 4 PoE Power over Ethernet classification providing 12.95–25.50 watts / 36–44 mA. Class 4 is not specified by 802.3af and therefore not supported by equipment supporting only 802.3af. 802.3at, commonly known as PoE+, defines Class 4. Class 4 devices are classified as High Power devices.

ClearVision Cisco ClearVision technology can take SD and ED video and reproduce the image at HD quality with no extra cost in bandwidth.

CMR Collaboration Meeting Rooms. Cisco's term for virtual conference meeting rooms accessed either through an SaaS or on-premises server.

CMR Cloud A Cisco CMR solution that can host WebEx users and video endpoints in the same collaboration meeting room hosted by WebEx Meeting Center.

CMR Hybrid A merger of the web-based CMR and on-premises Cisco TelePresence technologies that creates a single, seamless meeting experience whether attending via web or TelePresence endpoint.

Codec In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm used to compress/decompress speech or audio signals.

Collaboration Meeting Rooms (CMR) A WebEx cloud-based, persistent collaborative workspace enabling everyone to meet using nearly any device, for a business-quality video collaboration experience that combines video, voice, and content-sharing technologies.

Common Intermediate Format (CIF) An industry-standard video format representing a resolution of 288x352. This is the resolution used by PAL (European) television systems. Related resolutions are QCIF (Quarter CIF) and 4CIFl, which are 144x176 and 576x704, respectively. CIF is a 4:3 resolution full-screen.

Component video Component video takes the luminance and chrominance video data and sends out luminance, chrominance blue, chrominance red, and chrominance yellow or green on separate copper connections.

Composite video Composite video takes the luminance and chrominance video data and compresses it together to send across a singe copper connection.

Computer Telephony Integration (CTI) Computer Telephony Integration extends the rich feature set available on CUCM to third-party applications. At the desktop, Cisco CTI enables third-party applications to make calls from within Microsoft Outlook, open Windows, or start applications based on incoming caller ID and remotely track calls and contacts for billing purposes. Cisco CTI-enabled server applications can intelligently route contacts through an enterprise network, provide automated caller services such as auto-attendant and interactive voice response (IVR), and capture media for contact recording and analysis. For purposes of the exam, it is the mechanism that provides a means of providing desk phone control from a software client, such as Cisco Jabber.

Computer Telephony Interface (CTI) route point A virtual endpoint that, for DTMF purposes, supports all out-of-band (OOB) methods and does not support RFC 2833. CTI route points use CTI events to communicate with CTI-capable applications. For example, a CTI route point directs inbound calls to application services, such as a Unity Connection call handler or a Cisco Unified Contact Center Express or Enterprise IVR.

Computer Telephony Interface Quick Buffer Encoding (CTIQBE) Allows an extension to CTI for NAT/PAT, allowing telephony applications to function across a firewall.

Conference A virtual meeting space reserved for participants who are able to dial into it. Cisco refers to conferences as CMRs, or Collaboration Meeting Rooms.

ConferenceMe Client application downloaded from an MCU that allows participants to join a conference from their computers. The computer must have a microphone, speakers, a camera, and a display monitor.

CoS Class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In SNA subarea routing, CoS definitions are used by subarea nodes to determine the optimal route to establish a given session. A CoS definition consists of a virtual route number and a transmission priority field. Also called ToS.

CSS UCS Cisco Connected Safety and Security UCS Server.

CTMan Cisco TelePresence Manager, a tool used to schedule TelePresence endpoints in a multipoint conference meeting through an MCU.

CTS Cisco TelePresence endpoint.

DAS Direct-attached storage is computer storage that is directly attached to one computer or server and is not, without special support, directly accessible to other ones.

Device pool Device pools define sets of common characteristics for devices. The device pool structure supports the separation of user and location information. The device pool contains only device- and location-related information.

Device security profile To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. Only the security features that the selected device and protocol support display in the Security Profile Settings window.

DHCP Dynamic Host Configuration Protocol is a client/server protocol used to provide IP information to a device automatically.

DHCP Ack The permission sent from the DHCP server to the client authorizing the IP Information to be used.

DHCP Discovery Fist step in the DHCP process where a device requests IP information from a DHCP server.

DHCP Offer The IP information a DHCP server sends to an endpoint as an offer. This does not yet configure the endpoint with this information.

DHCP Request The acceptance of the IP information from the client that was offered by the DHCP server.

DHCPDISCOVER A client seeking DHCP services will broadcast a DHCPDISCOVER message on the local subnet to locate available DHCP server resources for that subnet. Servers respond with a DHCPOFFER message.

DHCPOFFER A message sent to an end station in response to that station's broadcast of a DHCPDISCOVER message requesting DHCP services. The DHCPOFFER includes an available network address and any configured options, such as Option 150 TFTP Server for collaboration endpoints.

Digital Media Designer (DMD) An application component within the Cisco Digital Media System that allows formatting and layout of content to be displayed via Cisco DMP endpoints.

Digital Media Manager (DMM) A web-based media management application allowing scheduling and publication of digital media content to desktop and digital signage displays.

Digital media player (DMP) IP-based hardware endpoints that play live or on-demand content, motion graphics, web pages, and other dynamic content to digital displays.

Digital Media System (DMS) A suite of applications allowing the management and delivery of video (live or on-demand) and dynamic application content to digital displays

Digital signal processor (DSP) Specialized hardware microprocessors architecturally optimized for specific purposes. In the case of Cisco PVDMs, these are optimized to deal with conversion of analog and digital signals to or from packetized voice. They also provide for MTP, conferencing, and transcoding service for CUCM-based endpoints.

Digital Signs A subsystem component of the Cisco Digital Media Suite architecture that provides a central management portal for control, provisioning, and delivery of video and application content to digital media player devices.

Directory number (DN) The phone number assigned to an endpoint. The DN is a construct consisting of the actual assigned number and the partition in which that number is placed. The combination of the two creates a unique combination within CUCM.

DMZ A demilitarized zone is a small network that exists between a main corporate network and the public Internet. It is used as an extra layer of security to prevent unauthorized users from accessing important data within an organization's main corporate network.

DN The directory number is the host part of the URI endpoints use when registering to the Cisco Unified CM. The domain is typically the IP address of the Cisco Unified CM but is unseen by users when calls are placed.

DNS A record A DNS record that resolves to the IP address of a specific end host.

DNS SRV record A service locator DNS record that resolves to an application or protocol specific service handler. For example, the _collab-edge._tcp.domain.com DNS SRV record would be used to point Internet-based Jabber endpoints to the Expressway-E address for firewall-traversal purposes.

Domain Name Service (DNS) A network-based service that provides name resolution to IP address. DNS architecture creates a hierarchical, distributed naming system for computers, services, and other network resources. DNS servers are typically created for both internal and external naming services.

DSCP Differentiated services code point.

DSP Digital signal processing refers to various techniques for improving the accuracy and reliability of digital communications.

Dual-tone multifrequency (DTMF) A telecommunication signaling system using the tones generated at two frequencies within the voice-frequency band over telephone lines between telephone equipment and other communications devices and switching centers.

DVI Digital Video Interface is a composite video connector that comes in three styles: DVI-D (digital for HD video), DVI-A (analog for SD video), and DVI-I (interlaced, could receive a DVI-D or DVI-A connection).

DVR Digital video recorder is a security system device that records the video from up to 16 surveillance cameras on a hard disk. The frame rate can be switched from real time to time lapse to save disk space.

Dynamic Host Configuration Protocol (DHCP) As defined in RFC 2131, DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

E1 CAS E1 Channel Associated Signaling uses bits within specific channels to convey framing, clocking, and signaling information. In E1 R2 implementations, there are 32 channels; 30 are used for voice or data. One of the additional channels (0) is used for frame sync, CRC4, and alarms, while the other (16) is used for signaling.

E1 PRI E1 PRI is an ISDN interface to primary rate access. E1 primary rate access consists of a single 64-kbps D channel plus 30 B channels for voice or data.

EP The recording times on a VHS cassette up to triple the time length using Extended Play (EP), also known as Super Long Play (SLP). By using LP or EP/SLP, the already poor quality is reduced.

Euroblock Audio connecter that uses a tap screw to attach raw audio wires.

Expressway-C The internal gateway component of the Cisco Expressway (Collaboration Edge) solution. Cisco Expressway-C and Expressway-E form a secure traversal link to enable video, voice, content, and IM&P services to software clients and endpoints outside the firewall.

Expressway-E The external gateway component of the Cisco Expressway (Collaboration Edge) solution. Cisco Expressway-C and Expressway-E form a secure traversal link to enable video, voice, content, and IM&P services to software clients and endpoints outside the firewall.

Extensible Messaging and Presence Protocol (XMPP) A standard protocol for message-oriented communications using an Extensible Markup Language (XML). XMPP is the underlying messaging protocol used by Cisco Jabber and numerous other IM clients.

External DNS DNS services located on the public Internet, usually maintained by a service provider.

FHD capacitive FHD stands for full high definition. Capacitive is a technology used in touchscreen devices that allows for the device to respond more easily to touch. Alternatively, resistive touchscreen technology has been used.

FindMe An option on the Cisco VCS that allows multiple endpoints to ring when the FindMe ID is dialed.

Firewall traversal A mechanism offered by Cisco VCS and Expressway architectures that allows for VPN-less access to enterprise resources from authorized clients. These services include IM, presence, voice, video, and more.

Firmware The underlying operating system and software components of collaboration endpoints.

fps Frames per second.

FQDN The fully qualified domain name is the domain on URI and URL addresses that must be qualified against a server. The most common use of FQDNs is in conjunction with a DNS. However, in SIP environments, the URI address must qualify the domain being used against the SIP server before devices are allowed to register.

Full HD Full high definition includes resolutions above 720p30. Most common full HD resolutions are 1080p30 and 720p60.

Fully qualified domain name (FQDN) The designation of a unique end system, which includes its hostname and domain so that it can be resolved via DNS. For example, mail.domain.com is the FQDN of the mail server for domain.com.

Gatekeeper A call control and CAC mechanism most often associated with H.323 voice and video implementations.

Gateway An H.323 entity that provides interoperability between the IP network and analog or digital endpoints.

GET A message type used by some protocols to request specific information from a network service. For example, an HTTP GET message would issue a request to a web server for a specific web page.

GRQ/GCF Gatekeeper Request is a RAS message used by endpoints to locate a gatekeeper to register to when discovery mode is configured as auto. Gatekeeper Confirm is a RAS message used by the gatekeeper to send its IP address to the endpoint so that the endpoint can attempt to register to it.

H.225 H.225 is the H.323 call setup communication sent between devices. H.225 used RAS and Q.931 protocols for sending and receiving information.

H.245 Once the Q.931 handshake between devices is complete, H.245 is used for capabilities exchange, master/slave negotiations, and opening logical channels (or ports). H.245 is also responsible for closing logical channels at the end of a call.

H.263 An ITU-T standard video compression format for low bit rate video communications. Standard image sizes specified by H.263 include SQCIF (128x96 pixels), QCIF (176x144), and CIF (352x288) resolutions.

H.264 Also known as MPEG4 Part 10 (AVC), it is a block-oriented, motion-compensation-based ITU-T standard format used in providing high-quality, low-bit-rate video and often is used for Internet streaming, Blu-ray, HDTV, and numerous other purposes.

H.265 Video-compression codec that offers a higher pixel saturation and better video communication using less bandwidth.

H.320 A general ITU-T recommendation for running multimedia over ISDN-based networks.

H.323 The IP communication standard created by the ITU (International Telecommunications Union) in circa 1984 for voice and video communication over IP. H.323 was based on of the H.320 standard for circuit-switched communication.

H.323 gatekeeper The central call control server for H.323 devices. The H.323 gatekeeper is often referred to as gatekeeper. The Cisco VCS is the only gatekeeper in Cisco's audio and video product line.

H.460.18/.19 The ITU standard for H.323 firewall and NAT traversal.

HD High-Definition video is video of higher resolution and quality than standard definition. There is no standardized meaning for high definition, but any video image with considerably more than 576 horizontal lines is considered high definition. HD resolutions start at 1280x720, with an aspect ratio of 16:9.

HDMI High-Definition Multimedia Interface connectors are used for high-definition composite video, stereo audio and sometimes power, all carried over a singe cable.

HTTP Hypertext Transfer Protocol is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web (WWW). Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text.

HTTPS Secure Hypertext Transfer Protocol is the use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering.

HyperText Transfer Protocol (HTTP) As defined in RFC 2616, HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. It is a generic, stateless protocol that can be used for many tasks beyond its use for hypertext, such as name servers and distributed object management systems, through extension of its request methods, error codes, and headers. HTTP can be used by newer endpoints to download configuration information and firmware in a similar fashion as is done with TFTP. IP Phones upgrade their firmware images using HTTP on port 6970 from TFTP services integrated into one or more call processing platforms. When HTTP is not available, the phones use TFTP.

ICANN Internet Cooperation for Assigned Names and Numbers.

ICE Interactive Connectivity Establishment, an IETF NAT-traversal solution.

IEEE Institute for Electrical and Electronic Engineers.

IETF Internet Engineering Task Force.

IIS Internet Information Services is used by TMS to allow the user interface to be accessed through a web interface.

IMTC International Multimedia Telecommunications Consortium.

Inactive load A fallback firmware image kept on some Cisco collaboration endpoints in case of corruption or failure of the active load.

Inline power Cisco inline power is a prestandard solution to provide power to phones, access points, and so on prior to the ratification of the 802.3 power standards. Cisco inline power was introduced in 2000 with the Catalyst line of switches. The 802.3af standard was adopted in 2003.

Instant Messaging (IM) Instant messaging is used for real-time communications via text-based chat. Cisco Jabber is a standards-based XMPP IM client.

Instant Messaging & Presence (IM&P) CUCM IM&P, formerly known as Cisco Unified Presence Server (CUPS), is the component within the Cisco collaboration architecture that provides for XMPP-based network-based presence capabilities, desktop application, and calendar integration, in addition to instant messaging services.

Institute of Electrical and Electronics Engineers (IEEE) IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.

Integrated Switch Digital Network (ISDN) A standard communications protocol for transmission of voice, video, data, and other network services over traditional PSTN circuits.

Internal DNS A DNS implementation inside an enterprise network that may include business-specific entries for name resolution not meant to be made available to external DNS services.

Internet Message Access Protocol (IMAP) IMAP allows client-based email applications to access remote services and servers. This includes not only email services but also voice messaging and numerous other applications.

Interworking gateway The interworking gateway allows for calls to connect between SIP and H.323 devices. The Cisco VCS is an interworking gateway.

IP television (IPTV) Use of an IP-based internetwork for purposes of streaming live or on-demand content to network endpoints

ISDN Integrated Services Digital Network is a form of communication over the circuit-switched network using V.35, PRI, or BRI lines.

Jabber Full UC A Cisco Jabber client (desktop or mobile) that is configured to provide the full feature set available to Jabber users, including IM, presence, voice, video, voice messaging, calendar integration, desktop phone control, web integration, application integration, and other capabilities.

Jabber ID (JID) The unique Jabber identifier of an end user. JIDs take on a format of id@domain.com.

Jabber IM&P A Cisco Jabber client (desktop or mobile) that is configured to provide only IM and presence services. In IM&P mode, the Jabber desktop client is still capable of providing CTI control of a Cisco collaboration desktop endpoint.

Jabber phone A Cisco Jabber client (desktop or mobile) that is configured to provide only voice service.

Key Expansion Module (KEM) A Key Expansion Module provides button expansion for some Cisco IP Phone models through the addition of one or more sidecar modules.

LCD Liquid crystal display television has better quality than a cathode ray tube (CRT) TV.

Light-emitting diode (LED) A two-lead semiconductor light source characterized by low power consumption, longer lifetime, improved resilience, and small size.

Lightweight Directory Access Protocol (LDAP) A client/server protocol meant to provide a mechanism for connecting to, searching, and modifying Internet directories.

Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) An IEEE standard protocol built specifically for voice applications. LLDP-MED is an extension of LLDP. It defines how a switch transitions from LLDP to LLDP-MED if an endpoint is detected. LLDP-MED is closely related to CDP and contains similar features and functions. LLDP-MED reports VLAN and power information but contains the ability to specify additional capabilities beyond those reported by CDP.

LLDP-MED Protocol used for VLAN discovery when the node, switch, or both are not Cisco devices.

LP Long Play extends the recording time on a VHS cassette by double the time.

Luminance Shading and depth.

MAC address Unique Identifier used by the Cisco Unified CM to identify the device when communication is initiated through the TFTP service.

MCU Multipoint control unit. MCU is an industry-wide term referring to a device that bridges multiple participants together within a single call.

MCU service prefix Registers to the VCS. Informs the VCS to route calls to the MCU that begin with this prefix, regardless of the following digits.

Media Access Control (MAC) address A physical, burned-in address on a network adapter that provides a unique identifier to network interfaces for purposes of communication on the physical network segment.

Media Experience Engine (MXE) A network appliance deployed in an enterprise video architecture that provides media-transformation and -adaptation services for recorded and live content. This includes transcoding and transrating capabilities.

Media resource Any resource made available for call through the Cisco Unified CM. Popular media resources include music-on-hold (MOH), voice bridges, and video bridges (or MCUs).

Media resource group A collection of media resources.

Media resource group list A collection of media resource groups.

Mobile and Remote Access (MRA) A core component of collaboration edge architecture (Expressway). MRA allows Cisco Jabber and other endpoints VPN-less registration, call control, provisioning, messaging, and presence services.

Multicast Sends (data) across a computer network to several users at the same time (one-to-many communication).

Multiplex Media Technology used in TIP to compress multiple RTP and RTCP packets into a single stream.

Multipoint Any conference that consists of three or more participants.

Multipoint control unit (MCU) A mission-specific hardware-based or software-based entity used for providing videoconferencing and audio conferencing bridging resources.

Multisite The option key on an endpoint that enables native multipoint conferences.

Multiway Call escalation to an MCU when a third participant is added to a call.

NAS Network-attached storage is a file server that connects to the network. A NAS device contains a slimmed-down operating system and file system and processes only I/O requests by supporting the popular file-sharing protocols, primarily CIFS for Windows and NFS for UNIX.

NAT Network Address Translation.

Nontraversal Call Any call that is not a traversal call. That is, the VCS processes only signaling traffic.

OBTP One button to push. A Cisco feature that enables users and endpoints to join a collaboration meeting room by a single click of a button.

One table mode A layout used on Cisco TelePresence servers that allows up to four participants in one immersive endpoint room to be displayed on a single monitor while in a call with another immersive endpoint. It is recommended that there be at least three other immersive endpoints in a single call before one table mode is used.

Option 150 An optional parameter configured within a DHCP scope that provides a TFTP server address to endpoints on the subnet served by that scope.

OSD The onscreen display is the monitor display on endpoint.

Owner In Cisco Unified CM 10.0 and later, an owner of a phone must be identified. Who the owner of a phone is can be specified under the owner user ID, or this setting can be changed to Anonymous (Public/Shared Space).

Owner user ID This setting identifies who the owner is of this phone.

Packet Voice Digital Module (PVDM) A module containing a varied density of DSP resources that is installed into an Integrated Services Router to provide media services such as packetization, conference bridging, MTP, transcoding, and more for IP telephony calls.

Partition A logical grouping of directory numbers. The partition coupled with the number itself creates a unique DN for the endpoints. A list of partitions is parsed in a calling search space when an endpoint dials a number or URI. Only numbers/URIs contained in a partition within the collective calling search space available to the device may be called from a given endpoint.

PAT Port Address Translation.

Phone button template When adding phones, you can assign one of these templates to the phones or create a new template. Creating and using templates provides a fast way to assign a common button configuration to a large number of phones.

Phone load name This setting is used to identify a specific firmware version the TFTP server is to use when a device tries to register.

PIP Picture-in-picture is a small picture used to display a local endpoint's camera image within the OSD of the far-end image that is being displayed. This is a great tool for adjusting the near-end camera so that participants are centered in the frame.

PKI Private Key Infrastructure is a method of an encryption handshake between two devices so that information can be sent securely between them.

Plasma Plasma TVs get their name because they use small cells of electrically charged gases. Plasma TVs offer better quality pictures than LCD TVs, but they are also more prone to burn-in.

PoE Power over Ethernet is a Cisco-developed technology (standardized by the IEEE) for wired Ethernet LANs that allows the electrical current necessary for the operation of each device to be carried by the data cables rather than by power cords. There are two standards for PoE available today: 802.3af and 802.3at.

POTS Plain old telephone network. POTS is voice-grade telephone service employing analog signal transmission over copper loops.

Prefix for MCU registration Differentiates between aliases assigned to conferences from aliases assigned to endpoints.

PRI E1 Primary Rate Interface, PRI links are divided into two categories. E1 PRIs are used all over the world except for North America and Japan. They have 30 B channels that use 64 kbps and 2 D channels that use 64 kbps.

PRI T1 Primary Rate Interface, PRI links are divided into two categories. T1 PRIs are used in North America and Japan. They have 23 B channels that use 64 kbps and 1 D channel that uses 64 kbps.

Private branch exchange (PBX) An on-premises telephone switch providing telephony services to analog or digital handsets, typically provided by the manufacturer of said PBX.

Private Class A network 10.0.0.0–10.255.255.255.

Private Class B network 176.16.0.0–176.31.255.255.

Private Class C network 192.168.0.0–192.168.255.255.

PSTN Public switched telephone network is the world's collection of interconnected voice-oriented public telephone networks, both commercial and government owned, operating over circuit-switched technologies.

PTZ Pan, tilt, zoom reflects the movement options of the camera.

Q.931 H.Q.931 is the H.323 call setup communication sent between devices. Q.931 exchanges source and destination IP addresses and any crypto-hash tokens between the devices. Q.931 also handles the alerting and connect messages sent from the destination device.

Quality of service (QoS) The capability of a network to provide differentiated services to specific types of network traffic to provide prioritization, dedicated bandwidth, controlled jitter and latency, and improved loss characteristics while ensuring that the prioritization does not cause one or more other traffic flows to fail.

RAS Registration, Admission, Status are communication messages sent between devices and an H.323 gatekeeper.

RCA RCA derives from Radio Corporation of America. These connectors are ungrounded for audio and composite for video. Low quality is to be expected when they are used, and they should not be used for distances that exceed 6 feet.

RCF Registration Confirm; part of the H.323 RAS messaging. Sent from the gatekeeper to an endpoint confirming registration was successful.

Real-time Transport Protocol (RTP) A standard for using UDP to transport real-time data, such as interactive voice/video over data networks.

Remote Desktop Protocol (RDP) Remote Desktop Protocol is used to control Microsoft Windows-based PCs and servers from remote destinations.

Rich Media Session (RMS) A Cisco Expressway license required for concurrent calls to/from any endpoint or application not registered to Cisco Unified Communications Manager. This includes business-to-business calls, Cisco Collaboration Meeting Rooms, Jabber guest, and interworked calls (for example, H.323 to SIP, H.264 AVC to H.264 SVC).

ROI Return on investment.

RRJ Registration Reject; part of the H.323 RAS messaging. Sent from the gatekeeper to an endpoint confirming registration was unsuccessful.

RRQ Registration Request; part of the H.323 RAS messaging. Sent from an endpoint to the gatekeeper to request registration.

RTCP Real-time Transport Control Protocol, used to send signaling packets over IP.

RTP Real-time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, time stamping, and delivery monitoring to real-time applications.

SaaS Software-as-a-service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

SAN Storage-area network is a dedicated high-speed network (or subnetwork) that interconnects and presents shared pools of storage devices to multiple servers.

SD Standard definition is a resolution that is not considered to be either high-definition television (1080i, 1080p, 1440p, 4K UHDTV, and 8K UHD) or enhanced-definition television (EDTV 480p).

SDES Secure Description is a protocol used to encrypt UDP media packets over RTP.

SDP Session Description Protocol is the process created by the IETF that allows devices to exchange their capabilities and desired ports for communication during call setup.

Secure Real-time Transport Protocol (SRTP) An implementation of RTP intended to provide encryption, message authentication and integrity, and protection from replay of RTP data.

Secure Shell password Cisco Technical Assistance Center (TAC) uses Secure Shell for troubleshooting and debugging. Contact TAC for further assistance.

Secure Shell user Cisco Technical Assistance Center (TAC) uses secure shell for troubleshooting and debugging. Contact TAC for further assistance.

Session Initiation Protocol (SIP) An IETF standard for multimedia calls over IP. SIP defines both line-side and trunk-side protocol specifications.

Show and Share A network-based application solution for video content authoring, management, storage, and publication/distribution.

Simple Object Access Protocol (SOAP) A messaging protocol that allows for disparate system communications via HTTP.

SIP Session Initiation Protocol. The IP communication protocol created by the IETF (Internet Engineering Task Force) circa 1985. SIP was originally created as a less-chatty way of sending IP packets across the internet before broadband and high-speed Internet was introduced. It was first used for VoIP calling in 1998 when Selcious came out with their Call Manager. They were bought by Cisco in 1999. SIP was first used for video communication circa 2006 by TANDBERG, who was bought by Cisco in 2010.

SIP 200 OK A message returned as part of a SIP call setup indicating that a particular request was accepted.

SIP profile SIP profiles change SIP incoming or outgoing messages so that interoperability between incompatible devices can be ensured. SIP profiles can be configured with rules to add, remove, copy, or modify the SIP Session Description Protocol (SDP).

SIP proxy The function of a SIP server used to connect, or proxy, calls signaling between two endpoints.

SIP Register A message sent by an endpoint requesting registration with a SIP registrar.

SIP registrar The function of a SIP server used to register endpoints to the SIP server. A table is created mapping the SIP URI with the endpoint's IP address.

SIP server The central call control server for SIP devices. The SIP server is sometimes referred to as the SIP proxy or SIP registrar, which are functions of the SIP server. The Cisco Unified CM and the Cisco VCS are both SIP servers.

Skinny Call Control Protocol (SCCP) A Cisco proprietary line-side signaling protocol designed for use with Cisco IP Phones.

SLA Service level agreement.

SLP Super Long Play, same thing as EP.

Smart Scheduler Tool accessed through TMS used to manage FindMe templates and schedule conferences. The application is intended for nontechnical employees within an organization.

SNMP Simple Network Management Protocol is used by TMS to manage systems.

Software development kit (SDK) Software development Kits are used in open development clients/applications, such as Cisco Jabber. The SDK can be used to create a highly version of the client for use in environments with special use cases or needs.

SPAN Switched Port Analyzer. SPAN is a feature that is available on switches based on Cisco IOS and NX-OS software that allows traffic received on a port or VLAN to be copied to another port for analysis. It is also referred to as port mirroring.

SQL Structured Query Language. Read/write database used by TMS to manage systems.

SRTP Secure Real-time Transport Protocol is the encrypted channel, or port, used to carry media data packets across a network.

SSH Secure Shell Protocol. Protocol that provides a secure remote connection to a router through a TCP application.

SSH access This setting is specific to the DX series endpoints. SSH access must be enabled for administrators to access the CLI of DX endpoints. The CLI allows access to important log information and allows administrators to issue certain commands for testing, configuring, and troubleshooting DX endpoints.

Static Assigning IP information to an endpoint manually, without using DHCP. An IP address, subnet mask, and default gateway address must be provided at a minimum.

STUN Session Traversal Utilities for NAT. IETF NAT-traversal solution.

Super resolution enhancement MCUs are able to generate higher-resolution images from SD and ED sources, greatly improving the clarity and detail of SD and ED sources in a call.

S-Video Separate Video, also known as S-Video, Super-Video, and Y/C, is a hybrid of composite and component video. It does not separate the blue, red, and green primary colors, but it does separate the luminance from the chrominance. Therefore S-Video generally has better resolution than composite video, but is not near as good as component video.

T1 CAS T1 Channel Associated Signaling, also known as robbed-bit signaling or in-band signaling, uses bits within individual channels to convey framing and clocking information. In T1 implementations, there are 24 such channels for voice or data.

T1 PRI T1 PRI is an ISDN interface to primary rate access. T1 primary rate access consists of a single 64-kbps D channel plus 23 B channels for voice or data.

TCP Transmission Control Protocol is used as a Layer 4 communication protocol that enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

TCS TelePresence Content Server. Recording and streaming server.

TelePresence Content Server (TCS) A network appliance used for recording and live streaming of video content.

TelePresence Management System (TMS) A network-based tool for provisioning, managing, and maintaining video endpoints and the scheduling and management of videoconference resources.

TFTP Trivial File Transfer Protocol is a file transfer protocol used to exchange information between systems. In a TelePresence environment, this tool is used to send endpoint configuration files to endpoint within a LAN network from the Cisco Unified CM.

TIP TelePresence Interoperability Protocol is used to multiplex audio and video streams into a single RTP and RTCP port.

TLS Transport Layer Security is a protocol used to encrypt TCP data packets.

TMS TelePresence Management Suite is management application software that runs on a Windows Server and manages TelePresence devices in a VCS-centric environment.

TMSPE TMS Provisioning Extension is an applet used by TMS to allow devices and users to be provisioned, FindMe templates to be provisioned, and it allows the use of the Smart Scheduler tool.

TMSXE TMS Exchange integration allows conferences to be scheduled through Microsoft Outlook.

Transmission Control Protocol (TCP) The connection-oriented transport protocol in the TCP/IP protocol suite.

Transmission Control Protocol/Internet Protocol (TCP/IP) A suite of protocols that allow for transmission of packets across an internetwork.

Traversal call Any call requiring VCS to pass call media and signaling. This might be a call from the inside of the network to the outside or vice versa. This also includes any interworking calls (H.323 <-> SIP or IPv4 <-> IPv6) calls wherein the endpoints are on opposite sides of a NAT implementation, any calls passing inbound on one LAN port and outbound on another for the same VCS (dual NIC), and all encrypted calls.

Trivial File Transfer Protocol (TFTP) A UDP-based file transfer protocol that requires no authentication. Cisco IP Phones use TFTP to download their firmware and configuration files. The address of the server is provided to the endpoint by the DHCP Option 150 parameter in the DHCP scope for the voice/video VLAN.

TURN Traversal Using Relays around NAT. IETF NAT-traversal solution.

UC Unified communications.

UCS Unified Computing System is an (x86) architecture data center server platform composed of computing hardware, virtualization support, switching fabric, and management software.

UDP User Datagram Protocol is commonly used for media and signaling after a call has been set up. UDP is a one-way communication.

Unicast Transmission of a data package or an audiovisual signal to a single recipient (one-to-one communication).

Unified Contact Center Enterprise (UCCE) A customer contact solution that delivers intelligent contact routing, call treatment, network-to-desktop computer telephony integration (CTI), and multichannel contact management over an IP infrastructure. It combines multichannel automatic call distributor (ACD) functionality with IP telephony in a unified solution that allows for scaling into the thousands of agents.

Unified Contact Center Express (UCCX) A sophisticated single-server (or dual with HA) customer contact solution that delivers call routing, comprehensive contact management, reporting, interactive voice response, and proactive customer service capabilities for up to 400 agents.

Universal device template (UDT) Templates that define all device-related settings in one simple interface and can be applied to any device. UDTs use tokens, which are variables in specific fields that fill in information (such as an employee name) automatically.

Universal line template (ULT) Templates that allow application of predefined settings that would normally be applied to a directory number.

Universal Port technology Cisco TelePresence MCU technology that allows each virtual port to be encoded and decoded independently.

Universal Resource Identifier (URI) An standard alphanumeric identifier used for dialing SIP endpoints rather than dialing via traditional telephone numbers. The SIP URI format is similar to that of an email address in that it includes both a unique user ID and a domain name (for example, user@cisco.com).

Universal Resource Locator (URL) The generic term for all types of names and addresses that refer to objects on the World Wide Web.

URI Uniform Resource Identifier. Type of formatted identifier that encapsulates the name of an Internet object and labels it with an identification of the name space, thus producing a member of the universal set of names in registered name spaces and of addresses referring to registered protocols or name spaces (RFC 1630).

User Data Services (UDS) A REST-based set of operations that provide authenticated access to user resources and entities such as user's devices, subscribed services, speed dials, and much more from the Unified Communications configuration database. UDS is available with CUCM 10.0 and later.

User Datagram Protocol (UDP) The connectionless transport protocol in the TCP/IP protocol suite.

V.35 V.35 is a high-speed serial interface the supports speeds in excess of 20 kbps. This serial interface allows for communication between Data Communication Equipment (DCE) and Data Terminal Equipment (DTE).

VCS Video Communications Server is a call control server for H.323 and SIP centered around video TelePresence. The VCS comes in two platforms: the VCS Control and the VCS Expressway.

VHS Video Home System is a widely adopted videocassette recording (VCR) technology that was developed by Japan Victor Company (JVC) and put on the market in 1976. It uses magnetic tape 1/2 inch (1.27 cm) in width.

Video Communications Server (VCS) Control A Cisco video call control element that provides flexible and extensible video calling/conferencing capabilities to endpoints within an enterprise. It peers with VCS Expressway to provide firewall-traversal capabilities for endpoints on the inside of the firewall needing to call endpoints outside of the enterprise network.

Video Communications Server (VCS) Expressway A Cisco video call control element that provides flexible and extensible video calling/conferencing capabilities to endpoints outside of an enterprise. It peers with the VCS Control to provide firewall-traversal capabilities for endpoints on the outside of the firewall needing to call endpoints on the inside of the enterprise network.

Virtual TelePresence Server (VTS) A software-based videoconferencing bridge used with CUCM to enable multiparty audio/videoconferencing, and content sharing.

VLAN Virtual local-area network, decouples network traffic so that quality of service can be implemented.

VoIP Voice over IP is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

VSM The Cisco Video Surveillance Manager (VSM) is the management and control plane for the Cisco video-surveillance solution components.

VTC Video telecommunication.

Web access This setting is specific to the DX series endpoints. Web Access must be enabled for administrators to access the web interface of DX endpoints. The web interface allows access to important log information.

WebEx Event Center A WebEx cloud based solution designed for large scale virtual events, such as Town Hall, Webinar, or other presentations that need to allow thousands of attendees with seamless platform, device, and TelePresence compatibility.

WebEx Meeting Center A WebEx cloud based solution for web, audio, and videoconferencing. Meeting Center provides a shared workspace accessible from any Mac, PC, smartphone, tablet, or even TelePresence endpoint.

WebEx Meetings Server An slightly scaled-down, on-premises version of the WebEx Meeting Center experience.

WebEx One-Click An ad hoc option that allows you to launch a WebEx meeting with a single click of a button.

WebEx Support Center A WebEx cloud-based platform designed to allow companies to offer remote technical support and live, personalized assistance for their customers.

WebEx Training Center A WebEx cloud based solution aimed at providing an interactive, highly customizable training platform for large scale online courses, online training, or other learning events.

WSVGA Wide-screen VGA offers resolutions of 1024x600 and 1024x576 to what would normally be a composite VGA connection.

XLR A grounded audio connector commonly used with commercial and professional equipment.

YPrPb Y is the luminance of a digital video feed; Pr and Pb are the primary red and primary blue chrominance of a video feed. The primary green is provided through an algorithm based on how much blue and red are used.

Index

Numerics

A

B

C

D

E

F

G

H

J

K

L

M

N

O

P

Q-R

S

T

U

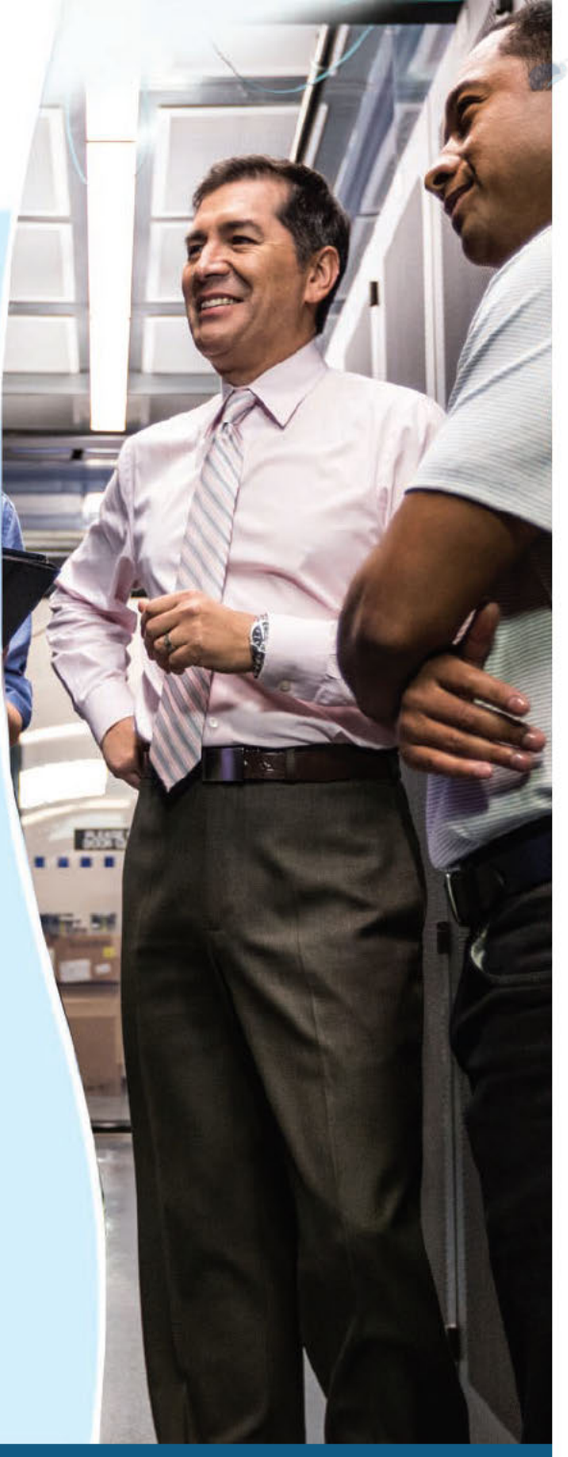
V

W

X-Y-Z

Connect, Engage, Collaborate

The Award Winning Cisco Support Community



Attend and Participate in Events

Ask the Experts
Live Webcasts

Knowledge Sharing

Documents
Blogs
Videos

Top Contributor Programs

Cisco Designated VIP
Hall of Fame
Spotlight Awards

Multi-Language Support

https://supportforums.cisco.com

Memory Tables

Chapter 2

Table 2-2 Cisco DMP Model Summary

	4400G	4310	300	340
Processor	1.5-GHz single core	667-MHz single core	1.2-GHz single core	1.6-GHz dual core
Memory				
Storage	4GB compact flash	32GB on-board	4GB Flash	32GB SSD and SD Port
USB Ports	2	2	4	4
Ethernet				
Wireless				
PoE				

Chapter 3

Table 3-3 Video-Surveillance Software Functions

Video-Surveillance Software	Video-Surveillance Software Functions
	Responsible for the recording, storing, and streaming of video feeds
	Offers centralized administration of all the Cisco video-surveillance solution components and supports Cisco video-surveillance endpoints
	Supports many layouts, and so operators can choose a predefined layout of cameras and push it out to the displays of all users, or choose to send different users various layouts with different camera feeds

Table 3-4 Cisco Storage Options

Cisco Storage Device	Storage Capacity	Type of Storage Available
Cisco Video Surveillance Multiservices Platform		
Cisco Integrated Services Router Generation 2		

Chapter 4

Table 4-2 Transport Circuit Options

Type	Data Channels	Special Channels	Geography
BRI			Global
T1 PRI			North America, Japan
T1 CAS			North America, Japan
E1 PRI			Europe, Australia, South America
E1 CAS			Europe, Australia, South America

Chapter 5

Table 5-2 Cisco 3905 IP Phone Features

Feature/Function	Characteristics
Integrated switch	
Display	128x32 monochrome LCD
Speakerphone	Yes
Line keys	
Programmable soft keys	
Fixed feature keys	8
MWI	Yes
XML support	
Headset port	No
Signaling protocol	
PoE class	

Table 5-3 Cisco 7800 Series Phone Features

Feature/Function	7821	7841	7861
Integrated switch			
Display	396x162-pixel backlit monochrome	396x162-pixel backlit monochrome	396x162-pixel backlit monochrome
Speakerphone	Yes	Yes	Yes
Line keys	2	4	16
Programmable soft keys	4	4	4
Fixed feature keys	11	11	11
Advanced features	Multicall per line Wideband audio EHS support (AUX port)	Multicall per line Wideband audio EHS support (AUX port) Gigabit Ethernet	Multicall per line Wideband audio EHS support (AUX port)
Hands-free	Yes	Yes	Yes
MWI	Yes	Yes	Yes
XML support	Yes	Yes	Yes
Signaling protocol			
802.3af	Yes	Yes	Yes
PoE class			
CUCM version	8.5.1 and later	8.5.1 and later	8.5.1 and later

C

Table 5-4 Cisco 7900 Wireless IP Phone Features

Feature/Function	7925G	7925G-EX	7926G
Display	2-inch 176x220-pixel color	2-inch digital, 16-bit graphical TFT color	2-inch digital, 16-bit graphical TFT color
Speakerphone	Yes	Yes	Yes
Line keys	N/A	N/A	N/A
Programmable soft keys			
Fixed feature keys	5	5	5
Advanced features	Bluetooth v2, push-to-talk via XML, Java MIDlet capabilities	Bluetooth v2, push-to-talk via XML, Java MIDlet capabilities, ATEX Zone 2 certification	Bluetooth v2, push-to-talk via XML, Java MIDlet capabilities, 2D barcode scanner

Feature/Function	7925G	7925G-EX	7926G
Hands-free	Yes	Yes	Yes
MWI	Yes	Yes	Yes
XML support			
Signaling protocol	Skinny Client Control Protocol (SCCP)	SCCP	SCCP
802.11a/b/g	Yes	Yes	Yes
CUCM version			

Table 5-5 Cisco 7942G and 7962G IP Phone Features

Feature/Function	7942G	7962G
Integrated switch		
Display	5-inch 320x222 4-bit grayscale	5-inch 320x222 4-bit grayscale
Speakerphone	Yes	Yes
Line keys		
Programmable soft keys	4 soft keys, 2 line keys (can be lines, speed dials, or programmable line keys)	4 soft keys, 6 line keys (can be lines, speed dials, or programmable line keys)
Fixed feature keys	10	10
Advanced features	High-resolution screen Application integration capabilities Headset hookswitch control	High-resolution screen Application integration capabilities Headset hookswitch control Up to 2 7915 expansion modules
Hands-free	Yes	Yes
MWI	Yes	Yes
XML support	Yes	Yes
Signaling protocol		
802.3af	Yes	Yes
PoE class	Class 2	Class 2
CUCM version	4.1 and later	4.1 and later

Table 5-6 Cisco 7945G, 7965G, and 7975G IP Phone Features

Feature/ Function	7945G	7965G	7975G
Integrated switch			
Display	5-inch 320x240 16-bit color, backlit	5-inch 320x240 16-bit color, backlit	5.6-inch 320x240 16-bit color, backlit touchscreen
Speakerphone	Yes	Yes	Yes
Line keys			
Programmable soft keys	4 soft keys, 2 line keys (can be lines, speed dials, or programmable line keys)	4 soft keys, 6 line keys (can be lines, speed dials, or programmable line keys)	5 soft keys, 8 line keys (can be lines, speed dials, or programmable line keys)
Fixed feature keys	10	10	10
Advanced features	High-resolution screen Application integration capabilities Headset hookswitch control	High-resolution screen Application integration capabilities Headset hookswitch control Up to 2 7915 or 7916 expansion modules	High-resolution screen Application integration capabilities Headset hookswitch control Up to 2 7915 or 7916 expansion modules
Hands-free	Yes	Yes	Yes
MWI	Yes	Yes	Yes
XML support	Yes	Yes	Yes
Signaling protocol			
802.3af	Yes	Yes	Yes
PoE class			
CUCM version	4.1 and later	4.1 and later	4.1 and later

Table 5-7 Cisco 8800 Series IP Phone Features

Feature/ Function	8811	8831	8841	8851	8861	8845	8865
Integrated switch							
Wireless capability							

Feature/ Function	8811	8831	8841	8851	8861	8845	8865
Display	5-inch 800x480 backlit mono-chrome		5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color
Speaker-phone	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Line keys							
Program-mable soft keys	4	4	4	4	4	4	4
Fixed feature keys	12	9	12	12	12	12	12
Integrated video	No	No	No	No	No	Yes – 720p HD, H.264 AVC, 80-deg FoV, privacy shutter	Yes – 720p HD, H.264 AVC, 80-deg FoV, 25-deg vertical tilt, privacy shutter
Advanced features							
Hands-free	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MWI	Yes	No	Yes	Yes	Yes	Yes	Yes
XML support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Signaling protocol							
802.3af	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PoE class							

Feature/ Function	8811	8831	8841	8851	8861	8845	8865
CUCM version	8.5(1) and later	7.1(5) and later	8.5(1) and later	8.5(1) and later	8.5(1) and later		

Table 5-8 Cisco 8900 Series IP Phone Features

Feature/Function	8945	8961
Integrated switch		
Display	5-inch 640x480 TFT, 24-bit color	5-inch 640x480 TFT, 24-bit color
Speakerphone	Yes	Yes
Line keys		
Programmable soft keys	4	4
Fixed feature keys	13	12
Advanced features		
Hands-free	Yes	Yes
MWI	Yes	Yes
XML support	Yes	Yes
Signaling protocol		
802.3af	Yes	Yes
PoE class		
CUCM version	7.1(5) and later	7.1(3) and later

Table 5-9 Cisco 9900 Series IP Phone Features

Feature/Function	9951	9971
Integrated switch		
Display	5-inch 640x480 TFT, 24-bit color	5.6-inch 640x480 TFT, 24-bit color
Speakerphone	Yes	Yes
Line/session keys		
Programmable soft keys	4	4
Fixed feature keys	12	12
Advanced features		
Hands-free	Yes	Yes
MWI	Yes	Yes
XML support	Yes	Yes
Signaling protocol		
802.3af	Yes	Yes
PoE class		
CUCM version	7.1(3)su1 and later	7.1(3)su1 and later

Table 5-10 Cisco EX Series Endpoint Features

Feature/Function	EX60	EX90
Integrated switch		
Display	21.5-inch LCD with LED backlight, 1920x1080, 170-degree viewing angle, 5-ms response	24-inch LCD with LED backlight, 1920x1200, 160-degree viewing angle, 5-ms response
Speakerphone	Yes	Yes
Camera		
Video standards	H.261 H.263 H.263+ H.264	H.261 H.263 H.263+ H.264

Feature/Function	EX60	EX90
Resolution	1920x1080 (16:9)	1920x1200 (16:10)
Signaling protocol		
TelePresence software version		
CUCM version	8.6(2) and later	8.6(2) and later

Table 5-11 Cisco DX650 Features

Feature/Function	DX650
Integrated switch	
Display	7-inch diagonal, backlit WSVGA capacitive touchscreen LCD with 1024x600-pixel resolution
Speakerphone	Yes
Camera	
Video standards	SIP only H.264 AVC
Resolution	WSVGA 1024x600
Signaling protocol	
CUCM version	7.1(5) and later

Chapter 6

Table 6-3 PoE Classes and Power Levels

Class	Wattage at PSE	Wattage at PD	Description
		0.44–12.94W	Default classification
		0.44–3.84W	Very low-power devices
		3.84–6.49W	Low-power devices
		6.49–12.95W	Mid-power devices
		12.95–25.50W	High-power devices

Table 6-4 Cisco Jabber Deployment Modes

Mode	IM	Presence	Telephony	Video
IM only				
Phone				
Full UC				

Table 6-5 Cisco Jabber DNS SRV Records

DNS SRV Record	DNS	Resolves To
_cisco-uds._tcp.domain.com		
_ cuplogin._tcp.domain.com		
_collab-edge._tls.domain.com		

Chapter 7

Table 7-2 CTS Endpoint Capabilities

Endpoint Name	Purpose	Number of Participants	Platform Options	Mounting Options
CTS 500	Personal office system			
CTS 1100	Multipurpose room system			
TX1300	Multipurpose room system			
TX9000	Immersive system			
IX5000	Immersive system			

Table 7-3 DX Series Endpoint Capabilities

Endpoint Name	Display	Front Camera	Operating System	Processor	Storage
DX650		High-definition video	Android 4.1.1	TI OMAP 4470 1.5 GHz	
DX70		High-definition video	Android 4.1.1	TI OMAP 4470 1.5 GHz	
DX80		High-definition video	Android 4.1.1	TI OMAP 4470 1.5 GHz	

Table 7-4 Current SX Endpoint Capabilities

Endpoint Name	Multisite	Audio Inputs	Audio Outputs	Video Inputs	Video Outputs
SX10		1 HDMI 1 minijack mic input 1 built-in mic	1 4-pin minijack 1 HDMI		
SX20		2 minijack mic input 1 minijack line in	1 minijack line out		
SX80		8 microphones EuroBlock connector 4 line-level EuroBlock 3 HDMI in (minijack)	6 line-level EuroBlock connector 2 HDMI		

Table 7-5 Current C Series Endpoint Capabilities

Endpoint Name	Multisite	Audio Inputs	Audio Outputs	Video Inputs	Video Outputs
C40				2 HDMI 1 DVI-I 1 composite	1 HDMI 1 DVI-I
C60				2 HDMI 2 DVI-I 1 composite	1 HDMI 1 DVI-I 1 composite
C90				4 HDMI 4 HD-SDI 2 DVI-I 2 YPbPr 1 S-video 1 composite	2 HDMI 2 DVI-I 1 composite

Table 7-6 Current EX Endpoint Capabilities

Endpoint Name	Screen Size/ Resolution	Multisite	DVI and HDMI Inputs	HDMI Outputs	Integrated Audio
EX60					
EX90					

Table 7-7 Current MX200 and MX 300 Endpoint Capabilities

Endpoint	Video Quality	Screen Size / Resolution / Contrast Ratio	DVI and HDMI Inputs	HDMI Outputs	Multisite Options
MX200			1 (PC) 0 (second source)	0	
MX200G2			1 (PC) 2 (second source)	1	
MX300			1 (PC) 0 (second source)	0	
MX300G2			1 (PC) 2 (second source)	1	

Table 7-8 Current MX700 and MX800 Endpoint Capabilities

Endpoint Name	Screen Size/ Resolution	Multisite	DVI and HDMI Inputs	DVI and HDMI Outputs	Audio Inputs
MX700					
MX800					

Chapter 9

Table 9-3 Phone Configuration Settings on the Cisco Unified CM

Phone Configuration Setting	Description	Required for Registration (Yes or No)
MAC address	Unique identifier used by the Cisco Unified CM to identify the device when communication is initiated through the TFTP service.	
Device pool	Device pools define sets of common characteristics for devices. The device pool structure supports the separation of user and location information. The device pool contains only device- and location-related information.	
Phone button template	When adding phones, you can assign one of these templates to the phones or create a new template. Creating and using templates provides a fast way to assign a common button configuration to a large number of phones.	
Calling search space (CSS)	Partitions can be seen as a collection of route patterns. DNs, route patterns, and translation patterns can all belong to specific partitions. Calling search spaces are an ordered list of route partitions, and they determine which partitions calling devices must search when they attempt to complete a call.	
Owner	In Cisco Unified CM Version 10.0 and later, an owner of a phone must be identified. Who the owner of a phone is can be specified under the owner user ID, or this setting can be changed to anonymous (public/shared space).	
Owner user ID	This setting identifies who the owner is of this phone.	
Phone load name	This setting is used to identify a specific firmware version the TFTP server is to use when a device tries to register.	
Allow control of device from CTI	The Computer Telephony Integration (CTI) control service on the Cisco Unified CM allows a phone to be controlled by the Jabber soft client, meaning that when Jabber sends or receives a call request, the media and signaling is rerouted through the associated phone.	
Device security profile	To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. Only the security features that the selected device and protocol support display in the Security Profile Settings window.	

Phone Configuration Setting	Description	Required for Registration (Yes or No)
SIP profile	SIP profiles change SIP incoming or outgoing messages so that interoperability between incompatible devices can be ensured. SIP profiles can be configured with rules to add, remove, copy, or modify the SIP Session Description Protocol (SDP).	
Secure Shell user	Cisco Technical Assistance Center (TAC) uses Secure Shell for troubleshooting and debugging. Contact TAC for further assistance.	
Secure Shell password	Cisco TAC uses secure shell for troubleshooting and debugging. Contact TAC for further assistance.	
Web access	This setting is specific to the DX series endpoints. Web access must be enabled for administrators to access the web interface of DX endpoints. The web interface allows access to important log information.	
SSH access	This setting is specific to the DX series endpoints. SSH access must be enabled for administrators to access the command-line interface (CLI) of DX endpoints. The CLI allows access to important log information and allows administrators to issue certain commands for testing, configuring, and troubleshooting DX endpoints.	

Chapter 10

Table 10-2 C90 Audio Calibration Options

Connector	Section	Options
	Unspecified	Default Volume
	Unspecified	Microphone Mute Enabled
	Unspecified	Volume
	Input	Level, Mode, Mute on Inactive Video, Video Input Source
	Input	Level, Mode, Mute on Inactive Video, Video Input Source
	Input	Channel, Level, Loop Suppression, Mode, Equalizer ID and Mode, Mute on Inactive Video, Video Input Source
	Input	Level, Mode, Type, Echo Control De-Reverberation Mode and Noise Reduction, Equalizer ID and Mode, Mute on Inactive Video, Video Input Source
	Output	Level, Mode
	Output	Level, Mode

Connector	Section	Options
	Output	Channel, Level, Mode, Type, Equalizer ID and Mode
	Sounds and Alerts	On, Off
	Sounds and Alerts	Ascent, Calculation, Delight, Evolve, Mellow, Mischief, Playful, Reflections, Ringer, Ripples, Sunrise, Vibes
	Sounds and Alerts	0–100

Table 10-3 C90 Video Calibration Options

Menu	Section	Options
Allow Web Snapshots	Unspecified	On, Off (Can only be configured from the remote control or CLI with a serial connection)
Default Presentation Source	Unspecified	1–5
Main Video Source	Unspecified	1–5
Monitors	Unspecified	Auto Single, Dual, Dual Presentation Only, Triple Presentation Only, Triple, Quadruple
Self-View	Unspecified	On, Off
Self-View Position	Unspecified	Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left Lower Right
Wallpaper	Unspecified	None, Custom, Growing, Summer Sky, Waves, Blue
Duration	CamCtrlPip CallSetup	1–60
Mode	CamCtrlPip CallSetup	On, Off
HDMI1–4 RGB Quantization Range	Input	
	Input	RGB Quantization Range, Type (Auto Detect, Digital, Analog RGB, Analog YPbPr)
Source 1–5	Input	Connector, Name, Presentation Selection, Quality, Type, Visibility, Camera ID, Mode, Optimal Definition Profile, Threshold 60 fps
Disable Disconnected Local Outputs	Layout	On, Off
Local Layout Family	Layout	

Menu	Section	Options
Presentation Default View	Layout	Default, Minimized, Maximized
Remote Layout Family	Layout	
Scale to Frame	Layout	
Scale to Frame Threshold	Layout	0–100
Scaling	Layout	On, Off
Auto Select Presentation Source	OSD	On, Off
Call Settings Selection	OSD	On, Off
Encryption Indicator	OSD	Auto, Always On, Always Off
Language Selection	OSD	On, Off
Login Required	OSD	On, Off
Menu Startup Mode	OSD	Home, Closed
Missed Calls Notification	OSD	On, Off
Mode	OSD	On, Off
My Contacts Expanded	OSD	On, Off
Output	OSD	Auto, 1-4
Today's Bookings	OSD	
Virtual Keyboard	OSD	User Selectable, Always On
Wallpaper Selection	OSD	On, Off
Input Method Cyrillic	OSD	On, Off
Input Language	OSD	Latin, Cyrillic
Composite 5	Output	Monitor Role, Over-Scan Level, Resolution, Location Horizontal Offset, Location Vertical Offset
DVI 2 and 4	Output	Monitor Role, Over-Scan Level, Resolution, RGB Quantization Range, Location Horizontal Offset, Location Vertical Offset
HDMI 1 and 3	Output	CEC Mode, Monitor Role, Over-Scan Level, Resolution, Location Horizontal Offset, Location Vertical Offset

Menu	Section	Options
	PIP	Current, Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left Lower Right
	PIP	Current, Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left Lower Right
Full Screen Mode	Self-View Default	Current, Off, On
Mode	Self-View Default	Current, Off, On
On Monitor Role	Self-View Default	
	Self-View Default	Current, Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left, Lower Right

Chapter 11

Table 11-2 Assent and H.460.18/.19 Ports Needed

Protocol	Assent	H.460.18 and H.460.19
RAS (UDP port)		
Q.931 (TCP port)		
H.245 (TCP port)		
RTP (UDP port)		
RTCP (UDP port)		

Table 11-3 Certificate Types Used in an Expressway Edge Solution

Certificate Type	Core	Edge	Comments
Public or enterprise certificate authority (CA) certificate chain to sign Expressway Core certificate			Required to establish traversal zone connection
Public or enterprise CA certificate chain to sign Expressway Edge certificate			Required to establish traversal zone connection
Cisco Unified CM Tomcat certificates or CA chain			Only required when Expressway Core configured to use TLS verify mode on Cisco Unified CM discovery
Cisco Unified CM CallManager certificates or CA chain			Only required when Cisco Unified CM is in mixed mode for end-to-end TLS

Certificate Type	Core	Edge	Comments
Cisco Unified CM IM and Presence Tomcat certificates or CA chain			Only required when Expressway Core configured to use TLS verify mode on IM and Presence discovery
Cisco Unified CM CAPF certificate or certificated			Only required when remote endpoints authenticate with a locally significant certificate (LSC)

Chapter 12

Table 12-2 Audio and Video Components

Audio Input Devices	Audio Output Devices	Video Input Devices	Video Output Devices

Table 12-3 Cisco TelePresence Codec C90 Video Input Ports

Video Input 1	Video Input 2	Video Input 3	Video Input 4	Video Input 5

Chapter 13

Table 13-2 Cisco Multipoint Solution Options

Cisco Multipoint Platform	Call Control Deployment Option	Primary Characteristics
Cisco TelePresence MCU	Cisco Unified CM Cisco VCS	
Cisco TelePresence Server	Cisco Unified CM Cisco VCS	

Table 13-3 Cisco TelePresence MCU Layouts, Families, and View Modes

Family Description	View Mode
Family 1: Gives prominence to one participant over others	
Family 2: Displays a single participant	
Family 3: Displays the four most active participants without seeing them scaled down to a small size if there are many other participants	
Family 4: Gives equal prominence to up to 20 conference contributors and is useful for a "role call" of active participants	
Family 5: Gives prominence to two participants in the center of the view while showing smaller panes of other participants above and below	

Table 13-4 Comparison Chart for TelePresence Servers and TelePresence MCUs

Feature	Virtual TelePresence Server	310/320 TelePresence Server	7010 TelePresence Server	8710 TelePresence Server	4500 MCU	5300 MCU	MSE 8510 Media 2 MCU
Auto-attendant							
Cascading							
WebEx-enabled TelePresence support							
Optimized conferencing							
TIP							

Chapter 14

Table 14-2 MCU Participant Statistics Information

Audio Media Statistics	Video Media Statistics	Content Media Statistics	Control
Received	**Received**	**Received**	**Received**
Receive Stream	Receive Stream	Receive Stream	RTCP Receive Address
			Receiver Reports
Encryption	Encryption	Encryption	Packet Loss Reported

Audio Media Statistics	Video Media Statistics	Content Media Statistics	Control
	Channel Bit Rate	Channel Bit Rate	Sender Reports
Received Energy	Received Bit Rate	Received Bit Rate	Other
Packets Received			
	Delay Applied for Lipsync	Packets Received	
	Packets Received		
		Frame Rate	
	Frame Rate	Frame Errors	
Transmit	**Transmit**	**Transmit**	**Transmit**
			RTCP Transmit Address
Transmit Address	Transmit Address	Transmit Address	Packets Sent
Encryption	Encryption	Encryption	
Packets Sent	Channel Bit Rate	Channel Bit Rate	
	Transmit bit Rate	Transmit bit Rate	
	Packets Sent	Packets Sent	
	Temporal / Spatial	Temporal / Spatial	

Chapter 15

Table 15-2 TelePresence Server Conference Configuration Options

Field	Field Description
Name	The name of the conference.
	The unique identifier used for dialing in to the conference.
PIN	Enter the unique PIN for the conference.
	Whether to register the conference with the numeric ID as the H.323 ID.
	Whether to register the conference with the numeric ID with the SIP registrar.
Conference Locked	Locks a conference.
Encryption	Whether encryption is optional or required for this conference.

Field	Field Description
	If your multiscreen endpoints support the one table feature, you can select whether to use one table mode automatically when the correct combination of endpoints or endpoint groups is in a conference (3 or 4 one table endpoints plus less than 6 other endpoints or endpoint groups). Options include Disabled, 4 Person Mode.
Content Channel	If enabled, the content is able to support an additional video stream, sent potentially to all connected endpoints, intended for showing content video. This content video is typically high-definition, low-frame-rate data such as a presentation formed of a set of slides. Such presentation data can be sourced by an endpoint specifically contributing a separate content video stream.
	Controls the AGC setting for this conference. Options include Use Default, Disabled, Enabled.

Chapter 16

Table 16-2 Ports Used by TMS

Service	Protocol	Port	Direction (Relative to TMS)	
			IN	Out
	TCP			
HTTPS	TCP			
Telnet	TCP			x
Telnet Chal.	TCP	57		x
Telnet PLCM	TCP	24		x
FTP	TCP			
SNMP	UDP	161	x	x
SNMP traps	UDP	162	x	x
SMTP	TCP	25		
LDAP	TCP			
LDAPS	TCP	636	x	x
TMS Agent	TCP			
Polycom GAB	TCP	3361	x	
Polycom	TCP	3601		x
Polycom	TCP	5001		
TMS Agent Admin	TCP			

Table 16-3 Reports Available on Cisco TMS

Main Menu Option	Submenu Options	Purpose
		The Bridge Utilization page contains reporting information on how much Cisco TMS-managed bridges are being used. The data is gathered from direct-managed TelePresence Servers and TelePresence MCUs only.
Call Detail Records	All Endpoints and MCUs Endpoints MCUs Content server Gateway Gatekeeper and VCS User CDR	
		Shows which billing codes are applied to conferences.
Conferences	Conference Statistics Resources Events Scheduling Interface Bridging Methods	Tracks conferences per user, type, and so on.
System	Ticketing Log Feedback Log Connection Error System Connection Authentication failure Boot FTP Audit Low Battery on Remote Control	
Network	Packet Loss Log Packet Loss Conference Bandwidth Usage Network History	
Return on Investment	Return on Investment Global Return on Investment Local	Return on Investment and C02 Savings calculate return on investment and environmental savings for your video equipment.

Main Menu Option	Submenu Options	Purpose
C02 Savings		Return on Investment and C02 Savings calculate return on investment and environmental savings for your video equipment.
		Any search can be stored and reused as a template.

Chapter 17

Table 17-2 Cisco WebEx Products and Features

Cisco WebEx Product	Cisco WebEx Feature
	Audio, HD video at 720p30, content sharing, file transfer, polling, remote desktop control
	A client-based application running on a PC that offers audio, HD video at 720p30, content sharing, and instant messaging through the WebEx cloud
	All the features of WebEx Meeting Center plus breakout sessions, emoticons, and an attentiveness tool
	All the features of WebEx Meeting Center plus a scheduling and follow-up tool and support for up to 3000 participants
	Full technical support with a quicker fault-resolution time using all the features of WebEx Meeting Center

Table 17-3 Cisco WebEx Meeting Center Features with Descriptions

Feature	Description
	Uses port 80 over HTTP and port 443 over HTTPS.
	Uses the H.264 video codec for high-quality 720p30 HD video at low bandwidth rates.
	Anyone in the meeting who holds the “WebEx ball” can share a file, share an application, or share your desktop through WebEx.
	Once participants share their desktops, another participant can take control of the desktop in a secure fashion after permissions have been granted.
	Up to 500 participants can join a fully licensed WebEx Meeting Center session.

Feature	Description
	Meetings can be recorded over WebEx. After the meeting has ended, the recording can be streamed for playback or downloaded and played back on-demand.
	Files and applications can be transferred to all participants within a WebEx session for download.

Memory Table Answer Key

Chapter 2

Table 2-2 Cisco DMP Model Summary

	4400G	4310	300	340
Processor	1.5-GHz single core	667-MHz single core	1.2-GHz single core	1.6-GHz dual core
Memory	1 GB	512 MB	2 GB	2 GB
Storage	4GB compact flash	32GB on-board	4GB Flash	32GB SSD and SD Port
USB Ports	2	2	4	4
Ethernet	10/100/1000	10/100	1x 10/100/1000 uplink, 4x 10/100 downlinks	10/100/1000
Wireless	802.11 b/g	N/A	802.11 b/g/n	802.11 a/b/g/n
PoE	—	802.3af	—	802.3af

Chapter 3

Table 3-3 Video-Surveillance Software Functions

Video-Surveillance Software	Video-Surveillance Software Functions
Cisco Video Surveillance Media Server	Responsible for the recording, storing, and streaming of video feeds
Cisco Video Surveillance Operations Manager	Offers centralized administration of all the Cisco video-surveillance solution components, and supports Cisco video-surveillance endpoints
Cisco Video Surveillance Virtual Matrix	Supports many layouts, and so operators can choose a predefined layout of cameras and push it out to the displays of all users, or choose to send different users various layouts with different camera feeds

Table 3-4 Cisco Storage Options

Cisco Storage Device	Storage Capacity	Type of Storage Available
Cisco Video Surveillance Multiservices Platform	Up to 24 TB	DAS
Cisco Integrated Services Router Generation 2	Up to 1 TB	DAS

Chapter 4

Table 4-2 Transport Circuit Options

Type	Data Channels	Special Channels	Geography
BRI	2 x 64 kbps (B)	1 x 16 kbps (D)	Global
T1 PRI	23 x 64 kbps (B)	1 x 64 kbps (D)	North America, Japan
T1 CAS	24 x 64 kbps	— (in-band signaling)	North America, Japan
E1 PRI	30 x 64 kbps (B)	2 x 64 kbps (framing and D)	Europe, Australia, South America
E1 CAS	30 x 64 kbps	2 x 64 kbps (framing and signaling)	Europe, Australia, South America

Chapter 5

Table 5-2 Cisco 3905 IP Phone Features

Feature/Function	Characteristics
Integrated switch	10/100
Display	128x32 monochrome LCD
Speakerphone	Yes
Line keys	1
Programmable soft keys	0
Fixed feature keys	8
MWI	Yes
XML support	No
Headset port	No
Signaling protocol	SIP
PoE class	Class 1

Table 5-3 Cisco 7800 Series Phone Features

Feature/Function	7821	7841	7861
Integrated switch	10/100	10/100/1000	10/100
Display	396x162-pixel backlit monochrome	396x162-pixel backlit monochrome	396x162-pixel backlit monochrome
Speakerphone	Yes	Yes	Yes
Line keys	2	4	16
Programmable soft keys	4	4	4
Fixed feature keys	11	11	11
Advanced features	Multicall per line Wideband audio EHS support (AUX port)	Multicall per line Wideband audio EHS support (AUX port) Gigabit Ethernet	Multicall per line Wideband audio EHS support (AUX port)
Hands-free	Yes	Yes	Yes
MWI	Yes	Yes	Yes
XML support	Yes	Yes	Yes
Signaling protocol	SIP	SIP	SIP
802.3af	Yes	Yes	Yes
PoE class	Class 1	Class 1	Class 1
CUCM version	8.5.1 and later	8.5.1 and later	8.5.1 and later

D

Table 5-4 Cisco 7900 Wireless IP Phone Features

Feature/Function	7925G	7925G-EX	7926G
Display	2-inch 176x220-pixel color	2-inch digital, 16-bit graphical TFT color	2-inch digital, 16-bit graphical TFT color
Speakerphone	Yes	Yes	Yes
Line keys	N/A	N/A	N/A
Programmable soft keys	2	2	2
Fixed feature keys	5	5	5
Advanced features	Bluetooth v2, push-to-talk via XML, Java MIDlet capabilities	Bluetooth v2, push-to-talk via XML, Java MIDlet capabilities, ATEX Zone 2 certification	Bluetooth v2, push-to-talk via XML, Java MIDlet capabilities, 2D barcode scanner

Feature/Function	7925G	7925G-EX	7926G
Hands-free	Yes	Yes	Yes
MWI	Yes	Yes	Yes
XML support	Yes	Yes	Yes
Signaling protocol	Skinny Client Control Protocol (SCCP)	SCCP	SCCP
802.11a/b/g	Yes	Yes	Yes
CUCM version	4.1 and later	4.1 and later	4.1 and later

Table 5-5 Cisco 7942G and 7962G IP Phone Features

Feature/Function	7942G	7962G
Integrated switch	10/100	10/100
Display	5-inch 320x222 4-bit grayscale	5-inch 320x222 4-bit grayscale
Speakerphone	Yes	Yes
Line keys	2 (lighted)	6 (lighted)
Programmable soft keys	4 soft keys, 2 line keys (can be lines, speed dials, or programmable line keys)	4 soft keys, 6 line keys (can be lines, speed dials, or programmable line keys)
Fixed feature keys	10	10
Advanced features	High-resolution screen Application integration capabilities Headset hookswitch control	High-resolution screen Application integration capabilities Headset hookswitch control Up to 2 7915 expansion modules
Hands-free	Yes	Yes
MWI	Yes	Yes
XML support	Yes	Yes
Signaling protocol	SCCP or SIP	SCCP or SIP
802.3af	Yes	Yes
PoE class	Class 2	Class 2
CUCM version	4.1 and later	4.1 and later

Table 5-6 Cisco 7945G, 7965G, and 7975G IP Phone Features

Feature/ Function	7945G	7965G	7975G
Integrated switch	10/100/1000	10/100/1000	10/100/1000
Display	5-inch 320x240 16-bit color, backlit	5-inch 320x240 16-bit color, backlit	5.6-inch 320x240 16-bit color, backlit touchscreen
Speakerphone	Yes	Yes	Yes
Line keys	2 (lighted)	6 (lighted)	8 (lighted)
Programmable soft keys	4 soft keys, 2 line keys (can be lines, speed dials, or programmable line keys)	4 soft keys, 6 line keys (can be lines, speed dials, or programmable line keys)	5 soft keys, 8 line keys (can be lines, speed dials, or programmable line keys)
Fixed feature keys	10	10	10
Advanced features	High-resolution screen Application integration capabilities Headset hookswitch control	High-resolution screen Application integration capabilities Headset hookswitch control Up to 2 7915 or 7916 expansion modules	High-resolution screen Application integration capabilities Headset hookswitch control Up to 2 7915 or 7916 expansion modules
Hands-free	Yes	Yes	Yes
MWI	Yes	Yes	Yes
XML support	Yes	Yes	Yes
Signaling protocol	SCCP or SIP	SCCP or SIP	SCCP or SIP
802.3af	Yes	Yes	Yes
PoE class	Class 3	Class 3	Class 3
CUCM version	4.1 and later	4.1 and later	4.1 and later

Table 5-7 Cisco 8800 Series IP Phone Features

Feature/ Function	8811	8831	8841	8851	8861	8845	8865
Integrated switch	10/100/ 1000	N/A	10/100/ 1000	10/100/ 1000	10/100/ 1000	10/100/ 1000	10/100/ 1000
Wireless capability	No	No	No	No	Yes – 802.11a/b/ g/n/ac	No	Yes – 802.11a/b/ g/n/ac

Feature/ Function	8811	8831	8841	8851	8861	8845	8865
Display	5-inch 800x480 backlit mono-chrome		5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color	5-inch 800x480 WVGA Color
Speaker-phone	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Line keys	5	1	5	5	5	5	5
Program-mable soft keys	4	4	4	4	4	4	4
Fixed feature keys	12	9	12	12	12	12	12
Integrated video	No	No	No	No	No	Yes – 720p HD, H.264 AVC, 80-deg FoV, privacy shutter	Yes – 720p HD, H.264 AVC, 80-deg FoV, 25-deg vertical tilt, privacy shutter
Advanced features	Gig Ethernet, wideband audio	Wired or wireless micro-phone kit, daisy-chain configura-tion	Gig Ethernet, wideband audio	Intelligent Proximity (Bluetooth hands-free pairing with smart-phone), USB smart-phone charging	Intelligent Proximity (Bluetooth hands-free pairing with smart-phone), USB smart-phone and tablet charging	Intelligent Proximity (Bluetooth hands-free pairing with smart-phone),	Intelligent Proximity (Bluetooth hands-free pairing with smartphone), USB smartphone and tablet charging
Hands-free	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MWI	Yes	No	Yes	Yes	Yes	Yes	Yes
XML support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Signaling protocol	SIP	SIP	SIP	SIP	SIP	SIP	SIP
802.3af	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PoE class	Class 2	Class 3	Class 2	Class 3	Class 4	Class 2	Class 4

Feature/ Function	8811	8831	8841	8851	8861	8845	8865
CUCM version	8.5(1) and later	7.1(5) and later	8.5(1) and later	8.5(1) and later	8.5(1) and later	CUCM: 8.5.1 (nonsecured mode), 8.6.2, 9.1.2, 10.0 and later Bus. Edition: 8.6.2, 9.1.2, 10.0 and later HCS: 8.6.2 and later	CUCM: 8.5.1 (nonsecured mode), 8.6.2, 9.1.2, 10.0 and later Bus. Edition: 8.6.2, 9.1.2, 10.0 and later HCS: 8.6.2 and later

Table 5-8 Cisco 8900 Series IP Phone Features

Feature/Function	8945	8961
Integrated switch	10/100/1000	10/100/1000
Display	5-inch 640x480 TFT, 24-bit color	5-inch 640x480 TFT, 24-bit color
Speakerphone	Yes	Yes
Line keys	4	5
Programmable soft keys	4	4
Fixed feature keys	13	12
Advanced features	Integrated camera, Bluetooth for headset connection	Gigabit Ethernet, wideband audio, XML/MIDlet support
Hands-free	Yes	Yes
MWI	Yes	Yes
XML support	Yes	Yes
Signaling protocol	SCCP or SIP	SIP
802.3af	Yes	Yes
PoE class	Class 2	Class 4
CUCM version	7.1(5) and later	7.1(3) and later

Table 5-9 Cisco 9900 Series IP Phone Features

Feature/Function	9951	9971
Integrated switch	10/100/1000	10/100/1000
Display	5-inch 640x480 TFT, 24-bit color	5.6-inch 640x480 TFT, 24-bit color
Speakerphone	Yes	Yes
Line/session keys	10	12
Programmable soft keys	4	4
Fixed feature keys	12	12
Advanced features	H.264 video, Bluetooth for headset, USB for headset, KEM support	H.264 video, Bluetooth for headset, USB for headset, KEM support, WiFi
Hands-free	Yes	Yes
MWI	Yes	Yes
XML support	Yes	Yes
Signaling protocol	SIP	SIP
802.3af	Yes	Yes
PoE class	Class 4	Class 4
CUCM version	7.1(3)su1 and later	7.1(3)su1 and later

Table 5-10 Cisco EX Series Endpoint Features

Feature/Function	EX60	EX90
Integrated switch	10/100/1000	10/100/1000
Display	21.5-inch LCD with LED backlight, 1920x1080, 170-degree viewing angle, 5-ms response	24-inch LCD with LED backlight, 1920x1200, 160-degree viewing angle, 5-ms response
Speakerphone	Yes	Yes
Camera	PrecisionHD, privacy shutter, document camera mode, 1/3-inch 2.1 mp, 50-degree horizontal / 29-degree vertical field of view	PrecisionHD, privacy shutter, document camera mode, optical motorized zoom, 1/3-inch 2.1 mp, 45-to 65-degree horizontal / 40- to 27-degree vertical field of view
Video standards	H.261 H.263 H.263+ H.264	H.261 H.263 H.263+ H.264

Feature/Function	EX60	EX90
Resolution	1920x1080 (16:9)	1920x1200 (16:10)
Signaling protocol	CUCM: SIP VCS: SIP/H.323	CUCM: SIP VCS: SIP/H.323
TelePresence software version	TC4.0 or TE6.0	TC3.1 or TE6.0
CUCM version	8.6(2) and later	8.6(2) and later

Table 5-11 Cisco DX650 Features

Feature/Function	DX650
Integrated switch	10/100/1000
Display	7-inch diagonal, backlit WSVGA capacitive touchscreen LCD with 1024x600-pixel resolution
Speakerphone	Yes
Camera	1080p, privacy shutter, 75-degree vertical / 67.4-degree horizontal field of view
Video standards	SIP only H.264 AVC
Resolution	WSVGA 1024x600
Signaling protocol	SIP
CUCM version	7.1(5) and later

Chapter 6

Table 6-3 PoE Classes and Power Levels

Class	Wattage at PSE	Wattage at PD	Description
0	Up to 15.4W	0.44–12.94W	Default classification
1	Up to 4W	0.44–3.84W	Very low-power devices
2	Up to 7W	3.84–6.49W	Low-power devices
3	Up to 15.4W	6.49–12.95W	Mid-power devices
4	Up to 30W (802.3at)	12.95–25.50W	High-power devices

Table 6-4 Cisco Jabber Deployment Modes

Mode	IM	Presence	Telephony	Video
IM only	Yes	Yes	No	No
Phone	No	No	Yes	Yes
Full UC	Yes	Yes	Yes	Yes

Table 6-5 Cisco Jabber DNS SRV Records

DNS SRV Record	DNS	Resolves To
_cisco-uds._tcp.domain.com	Internal	CUCM FQDN
_ cuplogin._tcp.domain.com	Internal	IM&P server FQDN
_collab-edge._tls.domain.com	External	VCS-E or Expressway-E FQDN

Chapter 7

Table 7-2 CTS Endpoint Capabilities

Endpoint Name	Purpose	Number of Participants	Platform Options	Mounting Options
CTS 500	Personal office system	1	1 32-inch monitor 1 manual camera	Pedestal Tabletop Wall mount
CTS 1100	Multipurpose room system	2	1 65-inch monitor 1 manual camera	Wall mount
TX1300	Multipurpose room system	6	1 65-inch monitor 3 manual cameras in cluster	Wall mount
TX9000	Immersive system	6 to 18	3 65-inch monitors 1 42-inch monitor 3 manual cameras in cluster	Purpose-built room
IX5000	Immersive system	6 to 18	3 70-inch monitors 3 auto cameras in cluster	Any-room system

Table 7-3 DX Series Endpoint Capabilities

Endpoint Name	Display	Front Camera	Operating System	Processor	Storage
DX650	7-inch backlit, Widescreen Super Video Graphics Array (WSVGA) capacitive touchscreen liquid crystal display (LCD) with 1024x600 pixel resolution	High-definition video	Android 4.1.1	TI OMAP 4470 1.5 GHz	1 GB RAM
DX70	14-inch backlit, full high definition (FHD) capacitive touchscreen LCD with 1920x1080 pixel resolution	High-definition video	Android 4.1.1	TI OMAP 4470 1.5 GHz	2 GB RAM
DX80	23-inch backlit, FDH capacitive touchscreen LCD with 1920x1080 pixel resolution	High-definition video	Android 4.1.1	TI OMAP 4470 1.5 GHz	2 GB RAM

Table 7-4 Current SX Endpoint Capabilities

Endpoint Name	Multisite	Audio Inputs	Audio Outputs	Video Inputs	Video Outputs
SX10	No	1 HDMI 1 minijack mic input 1 built-in mic	1 4-pin minijack 1 HDMI	1 HDMI 1 VGA	1 HDMI
SX20	576p 1+3	2 minijack mic input 1 minijack line in	1 minijack line out	1 HDMI 1 DVI-I	2 HDMI
SX80	1+4 at 720p30 1+3 at 1080p30	8 microphones EuroBlock connector 4 line-level EuroBlock 3 HDMI in (minijack)	6 line-level EuroBlock connector 2 HDMI	3 HDMI 1 DVI-I 1 BNC connector	2 HDMI 1 DVI-I

D

Table 7-5 Current C Series Endpoint Capabilities

Endpoint Name	Multisite	Audio Inputs	Audio Outputs	Video Inputs	Video Outputs
C40	576p 1+3	2 XLR 2 RCA/phono 1 HDMI	2 RCA/phono 1 HDMI	2 HDMI 1 DVI-I 1 composite	1 HDMI 1 DVI-I
C60	720p 1+3	4 XLR 2 RCA/phono 1 HDMI	2 RCA/phono 1 HDMI	2 HDMI 2 DVI-I 1 composite	1 HDMI 1 DVI-I 1 Composite
C90	1080p 1+3	8 XLR 4 RCA/phono 2 HDMI	2 XLR 4 RCA/phono 2 HDMI	4 HDMI 4 HD-SDI 2 DVI-I 2 YPbPr 1 S-video 1 composite	2 HDMI 2 DVI-I 1 composite

Table 7-6 Current EX Endpoint Capabilities

Endpoint Name	Screen Size/ Resolution	Multisite	DVI and HDMI Inputs	HDMI Outputs	Integrated Audio
EX60	21.5 inch 1920x1080	No	1 (PC) 0 (second source)	None	1 integrated microphone 2 integrated front speakers
EX90	24 inch 1920x1200	1080p 1+3	1 (PC) 1 (second source)	Dual display option, audio input and output	1 integrated microphone 2 integrated front speakers and subwoofer

Table 7-7 Current MX200 and MX 300 Endpoint Capabilities

Endpoint	Video Quality	Screen Size / Resolution / Contrast Ratio	DVI and HDMI Inputs	HDMI Outputs	Multisite Options
MX200	1080p30/720p60	42 inch 1920x1080 2500:1	1 (PC) 0 (second source)	0	No
MX200G2	1080p60/720p60	42 inch 1920x1080 1300:1	1 (PC) 2 (second source)	1	1+4 at 720p30 1+3 at 1080p30
MX300	1080p30/720p60	55 inch 1920x1200 5000:1	1 (PC) 0 (second source)	0	No
MX300G2	1080p60/720p60	55 inch 1920x1200 4000:1	1 (PC) 2 (second source)	1	1+4 at 720p30 1+3 at 1080p30

Table 7-8 Current MX700 and MX800 Endpoint Capabilities

Endpoint Name	Screen Size/ Resolution	Multisite	DVI and HDMI Inputs	DVI and HDMI Outputs	Audio Inputs
MX700	2x 55-inch 1920x1080	4+1 at 720p30 3+1 at 1080p30	3 HDMI 1 DVI-I	3 HDMI 1 DVI-I	15
MX800	70-inch 1920x1200	4+1 at 720p30 3+1 at 1080p30	3 HDMI 1 DVI-I	3 HDMI 1 DVI-I	15

Chapter 9

Table 9-3 Phone Configuration Settings on the Cisco Unified CM

Phone Configuration Setting	Description	Required for Registration (Yes or No)
MAC address	Unique identifier used by the Cisco Unified CM to identify the device when communication is initiated through the TFTP service.	Yes
Device pool	Device pools define sets of common characteristics for devices. The device pool structure supports the separation of user and location information. The device pool contains only device- and location-related information.	No
Phone button template	When adding phones, you can assign one of these templates to the phones or create a new template. Creating and using templates provides a fast way to assign a common button configuration to a large number of phones.	Yes
Calling search space (CSS)	Partitions can be seen as a collection of route patterns. DNs, route patterns, and translation patterns can all belong to specific partitions. Calling search spaces are an ordered list of route partitions, and they determine which partitions calling devices must search when they attempt to complete a call.	No
Owner	In Cisco Unified CM Version 10.0 and later, an owner of a phone must be identified. Who the owner of a phone is can be specified under the owner user ID, or this setting can be changed to anonymous (public/shared space).	Yes
Owner user ID	This setting identifies who the owner is of this phone.	No
Phone load name	This setting is used to identify a specific firmware version the TFTP server is to use when a device tries to register.	No
Allow control of device from CTI	The Computer Telephony Integration (CTI) control service on the Cisco Unified CM allows a phone to be controlled by the Jabber soft client, meaning that when Jabber sends or receives a call request, the media and signaling is rerouted through the associated phone.	No
Device security profile	To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. Only the security features that the selected device and protocol support display in the Security Profile Settings window.	Yes

Phone Configuration Setting	Description	Required for Registration (Yes or No)
SIP profile	SIP profiles change SIP incoming or outgoing messages so that interoperability between incompatible devices can be ensured. SIP profiles can be configured with rules to add, remove, copy, or modify the SIP Session Description Protocol (SDP).	Yes
Secure Shell user	Cisco Technical Assistance Center (TAC) uses Secure Shell for troubleshooting and debugging. Contact TAC for further assistance.	No
Secure Shell password	Cisco TAC uses secure shell for troubleshooting and debugging. Contact TAC for further assistance.	No
Web access	This setting is specific to the DX series endpoints. Web access must be enabled for administrators to access the web interface of DX endpoints. The web interface allows access to important log information.	No
SSH access	This setting is specific to the DX series endpoints. SSH access must be enabled for administrators to access the command-line interface (CLI) of DX endpoints. The CLI allows access to important log information and allows administrators to issue certain commands for testing, configuring, and troubleshooting DX endpoints.	No

Chapter 10

Table 10-2 C90 Audio Calibration Options

Connector	Section	Options
	Unspecified	Default Volume
	Unspecified	Microphone Mute Enabled
	Unspecified	Volume
HDMI3	Input	Level, Mode, Mute on Inactive Video, Video Input Source
HDMI4	Input	Level, Mode, Mute on Inactive Video, Video Input Source
Line 1–4 (RCA)	Input	Channel, Level, Loop Suppression, Mode, Equalizer ID and Mode, Mute on Inactive Video, Video Input Source
Microphone 1–8	Input	Level, Mode, Type, Echo Control De-Reverberation Mode and Noise Reduction, Equalizer ID and Mode, Mute on Inactive Video, Video Input Source
HDMI1	Output	Level, Mode
HDMI3	Output	Level, Mode

Connector	Section	Options
Line 1–4 (RCA)	Output	Channel, Level, Mode, Type, Equalizer ID and Mode
Key Tones Mode	Sounds and Alerts	On, Off
Ring Tone	Sounds and Alerts	Ascent, Calculation, Delight, Evolve, Mellow, Mischief, Playful, Reflections, Ringer, Ripples, Sunrise, Vibes
Ring Volume	Sounds and Alerts	0–100

Table 10-3 C90 Video Calibration Options

Menu	Section	Options
Allow Web Snapshots	Unspecified	On, Off (Can only be configured from the remote control or CLI with a serial connection)
Default Presentation Source	Unspecified	1–5
Main Video Source	Unspecified	1–5
Monitors	Unspecified	Auto Single, Dual, Dual Presentation Only, Triple Presentation Only, Triple, Quadruple
Self-View	Unspecified	On, Off
Self-View Position	Unspecified	Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left Lower Right
Wallpaper	Unspecified	None, Custom, Growing, Summer Sky, Waves, Blue
Duration	CamCtrlPip CallSetup	1–60
Mode	CamCtrlPip CallSetup	On, Off
HDMI1–4 RGB Quantization Range	Input	Auto, Full, Limited
DVI 3, 5	Input	RGB Quantization Range, Type (Auto Detect, Digital, Analog RGB, Analog YPbPr)
Source 1–5	Input	Connector, Name, Presentation Selection, Quality, Type, Visibility, Camera ID, Mode, Optimal Definition Profile, Threshold 60 fps
Disable Disconnected Local Outputs	Layout	On, Off
Local Layout Family	Layout	Auto, Full Screen, Equal, Presentation Small Speaker, Presentation Large Speaker, Prominent, Overlay, Single

Menu	Section	Options
Presentation Default View	Layout	Default, Minimized, Maximized
Remote Layout Family	Layout	Auto, Full Screen, Equal, Presentation Small Speaker, Presentation Large Speaker, Prominent, Overlay, Single
Scale to Frame	Layout	Manual, Maintain Aspect Ratio, Stretch to Fit
Scale to Frame Threshold	Layout	0–100
Scaling	Layout	On, Off
Auto Select Presentation Source	OSD	On, Off
Call Settings Selection	OSD	On, Off
Encryption Indicator	OSD	Auto, Always On, Always Off
Language Selection	OSD	On, Off
Login Required	OSD	On, Off
Menu Startup Mode	OSD	Home, Closed
Missed Calls Notification	OSD	On, Off
Mode	OSD	On, Off
My Contacts Expanded	OSD	On, Off
Output	OSD	Auto, 1-4
Today's Bookings	OSD	On, Off
Virtual Keyboard	OSD	User Selectable, Always On
Wallpaper Selection	OSD	On, Off
Input Method Cyrillic	OSD	On, Off
Input Language	OSD	Latin, Cyrillic
Composite 5	Output	Monitor Role, Over-Scan Level, Resolution, Location Horizontal Offset, Location Vertical Offset
DVI 2 and 4	Output	Monitor Role, Over-Scan Level, Resolution, RGB Quantization Range, Location Horizontal Offset, Location Vertical Offset
HDMI 1 and 3	Output	CEC Mode, Monitor Role, Over-Scan Level, Resolution, Location Horizontal Offset, Location Vertical Offset

Menu	Section	Options
Active Speaker Default Value Position	PIP	Current, Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left Lower Right
Presentation Default Value Position	PIP	Current, Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left Lower Right
Full Screen Mode	Self-View Default	Current, Off, On
Mode	Self-View Default	Current, Off, On
On Monitor Role	Self-View Default	First, Second, Current, Third, Fourth
PIP Position	Self-View Default	Current, Upper Left, Upper Center, Upper Right, Center Left, Center Right, Lower Left, Lower Right

Chapter 11

Table 11-2 Assent and H.460.18/.19 Ports Needed

Protocol	Assent	H.460.18 and H.460.19
RAS (UDP port)	1719	1719
Q.931 (TCP port)	2776	1720
H.245 (TCP port)		2777
RTP (UDP port)	2776	2776
RTCP (UDP port)	2777	2777

Table 11-3 Certificate Types Used in an Expressway Edge Solution

Certificate Type	Core	Edge	Comments
Public or enterprise certificate authority (CA) certificate chain to sign Expressway Core certificate	Y	Y	Required to establish traversal zone connection
Public or enterprise CA certificate chain to sign Expressway Edge certificate	Y	Y	Required to establish traversal zone connection
Cisco Unified CM Tomcat certificates or CA chain	Y	N	Only required when Expressway Core configured to use TLS verify mode on Cisco Unified CM discovery
Cisco Unified CM CallManager certificates or CA chain	Y	N	Only required when Cisco Unified CM is in mixed mode for end-to-end TLS

Certificate Type	Core	Edge	Comments
Cisco Unified CM IM and Presence Tomcat certificates or CA chain	Y	N	Only required when Expressway Core configured to use TLS verify mode on IM and Presence discovery
Cisco Unified CM CAPF certificate or certificated	N	Y	Only required when remote endpoints authenticate with a locally significant certificate (LSC)

Chapter 12

Table 12-2 Audio and Video Components

Audio Input Devices	Audio Output Devices	Video Input Devices	Video Output Devices
Microphones (MIC level)	Speakers (free standing)	Cameras	TVs
Microphones (Line level)	Active amplifiers	Computers	Monitors
Mixers	Passive amplifiers	Document camera	Projectors
Echo cancellation	Speakers (built in to monitor)	Video-playback device (DVR, DVD, Blu-ray)	

Table 12-3 Cisco TelePresence Codec C90 Video Input Ports

Video Input 1	Video Input 2	Video Input 3	Video Input 4	Video Input 5
HDMI 1	HDMI 2	HDMI 3	HDMI 4	HDMI 5
HD-SDI 1	HD-SDI 2	HD-SDI 3	HD-SDI 4	Composite 5
YPrPb 1	YPrPb 2	DVI 3	—	YC 5

Chapter 13

Table 13-2 Cisco Multipoint Solution Options

Cisco Multipoint Platform	Call Control Deployment Option	Primary Characteristics
Cisco TelePresence MCU	Cisco Unified CM Cisco VCS	Hardware video bridge for nonimmersive endpoints
Cisco TelePresence Server	Cisco Unified CM Cisco VCS	Hardware or software bridge for immersive and nonimmersive endpoints

Table 13-3 Cisco TelePresence MCU Layouts, Families, and View Modes

Family Description	View Mode
Family 1: Gives prominence to one participant over others	Enhanced Continuous Presence
Family 2: Displays a single participant	Active Speaker
Family 3: Displays the four most active participants without seeing them scaled down to a small size if there are many other participants	Enhanced Continuous Presence
Family 4: Gives equal prominence to up to 20 conference contributors, and is useful for a "role call" of active participants	Continuous Presence
Family 5: Gives prominence to two participants in the center of the view while showing smaller panes of other participants above and below	Enhanced Continuous Presence

Table 13-4 Comparison Chart for TelePresence Servers and TelePresence MCUs

Feature	Virtual TelePresence Server	310/320 TelePresence Server	7010 TelePresence Server	8710 TelePresence Server	4500 MCU	5300 MCU	MSE 8510 Media 2 MCU
Auto-attendant					Yes	Yes	Yes
Cascading					Yes	Yes	Yes
WebEx-enabled TelePresence support			Yes	Yes	Yes	Yes	Yes
Optimized conferencing	Yes	Yes	Yes	Yes			
TIP	Yes	Yes	Yes	Yes			

Chapter 14

Table 14-2 MCU Participant Statistics Information

Audio Media Statistics	Video Media Statistics	Content Media Statistics	Control
Received	**Received**	**Received**	**Received**
Receive Stream	Receive Stream	Receive Stream	RTCP Receive Address
Receive Address	Receive Address	Receive Address	Receiver Reports
Encryption	Encryption	Encryption	Packet Loss Reported

Audio Media Statistics	Video Media Statistics	Content Media Statistics	Control
Received Jitter	Channel Bit Rate	Channel Bit Rate	Sender Reports
Received Energy	Received Bit Rate	Received Bit Rate	Other
Packets Received	Received Jitter	Received Jitter	
Packet Errors	Delay Applied for Lipsync	Packets Received	
Frame Errors	Packets Received	Packet Errors	
	Packet Errors	Frame Rate	
	Frame Rate	Frame Errors	
	Frame Errors		
Transmit	**Transmit**	**Transmit**	**Transmit**
Transmit Stream	Transmit Stream	Transmit Stream	RTCP Transmit Address
Transmit Address	Transmit Address	Transmit Address	Packets Sent
Encryption	Encryption	Encryption	
Packets Sent	Channel Bit Rate	Channel Bit Rate	
	Transmit bit Rate	Transmit bit Rate	
	Packets Sent	Packets Sent	
	Frame Rate	Frame Rate	
	Temporal / Spatial	Temporal / Spatial	

Chapter 15

Table 15-2 TelePresence Server Conference Configuration Options

Field	Field Description
Name	The name of the conference.
Numeric ID	The unique identifier used for dialing in to the conference.
PIN	Enter the unique PIN for the conference.
Register Numeric ID with H.323 Gatekeeper	Whether to register the conference with the numeric ID as the H.323 ID.
Register Numeric ID with SIP registrar	Whether to register the conference with the numeric ID with the SIP registrar.
Conference Locked	Locks a conference.
Encryption	Whether encryption is optional or required for this conference.

Field	Field Description
Use One Table Mode When Appropriate	If your multiscreen endpoints support the one table feature, you can select whether to use one table mode automatically when the correct combination of endpoints or endpoint groups is in a conference (3 or 4 one table endpoints plus less than 6 other endpoints or endpoint groups). Options include Disabled, 4 Person Mode.
Content Channel	If enabled, the content is able to support an additional video stream, sent potentially to all connected endpoints, intended for showing content video. This content video is typically high definition, low-frame-rate data such as a presentation formed of a set of slides. Such presentation data can be sourced by an endpoint specifically contributing a separate content video stream.
Automatic Gain Control	Controls the AGC setting for this conference. Options include Use Default, Disabled, Enabled.

Chapter 16

Table 16-2 Ports Used by TMS

Service	Protocol	Port	Direction (Relative to TMS)	
			IN	Out
HTTP	TCP	80	x	x
HTTPS	TCP	443	x	x
Telnet	TCP	23		x
Telnet Chal.	TCP	57		x
Telnet PLCM	TCP	24		x
FTP	TCP	20, 21		x
SNMP	UDP	161	x	x
SNMP traps	UDP	162	x	x
SMTP	TCP	25		x
LDAP	TCP	389	x	x
TMS Agent	TCP	8989	x	x
Polycom GAB	TCP	3361	x	
Polycom	TCP	3601		x
Polycom	TCP	5001		x
TMS Agent Admin	TCP	4444	x	x

Table 16-3 Reports Available on Cisco TMS

Main Menu Option	Submenu Options	Purpose
Bridge Utilization		The Bridge Utilization page contains reporting information on how much Cisco TMS-managed bridges are being used. The data is gathered from direct-managed TelePresence Servers and TelePresence MCUs only.
Call Detail Records	All Endpoints and MCUs Endpoints MCUs Content server Gateway Gatekeeper and VCS User CDR	Tracks the frequency and duration of calls in your TelePresence deployment.
Billing Code Statistics		Shows which billing codes are applied to conferences.
Conferences	Conference Statistics Resources Events Scheduling Interface Bridging Methods	Tracks conferences per user, type, and so on.
System	Ticketing Log Feedback Log Connection Error System Connection Authentication Failure Boot FTP Audit Low Battery on Remote Control	Catches errors and other events from systems.
Network	Packet Loss Log Packet Loss Conference Bandwidth Usage Network History	Statistics reports on network and bandwidth usage.
Return on Investment	Return on Investment Global Return on Investment Local	Return on Investment and C02 Savings calculate return on investment and environmental savings for your video equipment.

Main Menu Option	Submenu Options	Purpose
C02 Savings		Return on Investment and C02 Savings calculate return on investment and environmental savings for your video equipment.
Reporting Template		Any search can be stored and reused as a template.

Chapter 17

Table 17-2 Cisco WebEx Products and Features

Cisco WebEx Product	Cisco WebEx Feature
WebEx Meeting Center	Audio, HD video at 720p30, content sharing, file transfer, polling, remote desktop control
WebEx Connect IM	A client-based application running on a PC that offers audio, HD video at 720p30, content sharing, and instant messaging through the WebEx cloud
WebEx Training Center	All the features of WebEx Meeting Center plus breakout sessions, emoticons, and an attentiveness tool
WebEx Event Center	All the features of WebEx Meeting Center plus a scheduling and follow-up tool, and support for up to 3000 participants
WebEx Support Center	Full technical support with a quicker fault-resolution time using all the features of WebEx Meeting Center

Table 17-3 Cisco WebEx Meeting Center Features with Descriptions

Feature	Description
TCP communication	Uses port 80 over HTTP and port 443 over HTTPS.
HD video	Uses the H.264 video codec for high-quality 720p30 HD video at low bandwidth rates.
Content sharing	Anyone in the meeting who holds the “WebEx ball” can share a file, share an application, or share your desktop through WebEx.
Remote desktop control	Once participants share their desktops, another participant can take control of the desktop in a secure fashion after permissions have been granted.
Participant capacity	Up to 500 participants can join a fully licensed WebEx Meeting Center session.

Feature	Description
Recording	Meetings can be recorded over WebEx. After the meeting has ended, the recording can be streamed for playback, or downloaded and played back on-demand.
File transfer	Files and applications can be transferred to all participants within a WebEx session for download.

Appendix E

Study Planner

Practice Test	Reading	Task
Labs and Exercises	Video	

Element	Task	Goal Date	First Date Completed	Second Date Completed (Optional)	Notes
Introduction	Read Introduction				
1. Introduction to Cisco Video Communications	Read Foundation Topics				
1 .Introduction to Cisco Video Communications	Review Key Topics				
1 .Introduction to Cisco Video Communications	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 1 in practice test software				
2. Cisco Digital Media and Content Delivery	Read Foundation Topics				
2. Cisco Digital Media and Content Delivery	Review Key Topics				
2. Cisco Digital Media and Content Delivery	Define Key Terms				
2. Cisco Digital Media and Content Delivery	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 2 in practice test software				
3. Describing Cisco Video Surveillance	Read Foundation Topics				
3. Describing Cisco Video Surveillance	Review Key Topics				
3. Describing Cisco Video Surveillance	Define Key Terms				
3. Describing Cisco Video Surveillance	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 3 in practice test software				

4. Cisco Collaboration Overview	Read Foundation Topics				
4. Cisco Collaboration Overview	Review Key Topics				
4. Cisco Collaboration Overview	Define Key Terms				
4. Cisco Collaboration Overview	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 4 in practice test software				
5. Cisco IP Phones, Desk Endpoints, and Jabber Overview	Read Foundation Topics				
5. Cisco IP Phones, Desk Endpoints, and Jabber Overview	Review Key Topics				
5. Cisco IP Phones, Desk Endpoints, and Jabber Overview	Define Key Terms				
5. Cisco IP Phones, Desk Endpoints, and Jabber Overview	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 5 in practice test software				
6. Configuring Cisco Unified IP Phones and Cisco Jabber	Read Foundation Topics				
6. Configuring Cisco Unified IP Phones and Cisco Jabber	Review Key Topics				
6. Configuring Cisco Unified IP Phones and Cisco Jabber	Define Key Terms				
6. Configuring Cisco Unified IP Phones and Cisco Jabber	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 6 in practice test software				
7. Describing Cisco TelePresence Endpoint Characteristics					
7. Describing Cisco TelePresence Endpoint Characteristics	Review Key Topics				
7. Describing Cisco TelePresence Endpoint Characteristics	Define Key Terms				
7. Describing Cisco TelePresence Endpoint Characteristics	Complete memory tables in Appendix C for this chapter				

Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 7 in practice test software				
8. Configuring Cisco TelePresence CTS Software-Based Endpoints	Read Foundation Topics				
8. Configuring Cisco TelePresence CTS Software-Based Endpoints	Review Key Topics				
8. Configuring Cisco TelePresence CTS Software-Based Endpoints	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 8 in practice test software				
9. Configuring Cisco DX Series Endpoints	Read Foundation Topics				
9. Configuring Cisco DX Series Endpoints	Review Key Topics				
9. Configuring Cisco DX Series Endpoints	Define Key Terms				
9. Configuring Cisco DX Series Endpoints	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 9 in practice test software				
10. Configuring Cisco TelePresence TC Software-Based Endpoints	Read Foundation Topics				
10. Configuring Cisco TelePresence TC Software-Based Endpoints	Review Key Topics				
10. Configuring Cisco TelePresence TC Software-Based Endpoints	Define Key Terms				
10. Configuring Cisco TelePresence TC Software-Based Endpoints	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 10 in practice test software				
11. Cisco Legacy Edge Architecture	Read Foundation Topics				
11. Cisco Legacy Edge Architecture	Review Key Topics				
11. Cisco Legacy Edge Architecture	Define Key Terms				

11. Cisco Legacy Edge Architecture	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 11 in practice test software				
12. Operating and Troubleshooting Cisco TelePresence Endpoints	Read Foundation Topics				
12. Operating and Troubleshooting Cisco TelePresence Endpoints	Review Key Topics				
12. Operating and Troubleshooting Cisco TelePresence Endpoints	Define Key Terms				
12. Operating and Troubleshooting Cisco TelePresence Endpoints	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 12 in practice test software				
13. Cisco Multipoint Solution	Read Foundation Topics				
13. Cisco Multipoint Solution	Review Key Topics				
13. Cisco Multipoint Solution	Define Key Terms				
13. Cisco Multipoint Solution	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 13 in practice test software				
14. Cisco TelePresence MCUs	Read Foundation Topics				
14. Cisco TelePresence MCUs	Review Key Topics				
14. Cisco TelePresence MCUs	Define Key Terms				
14. Cisco TelePresence MCUs	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 14 in practice test software				
15. Cisco TelePresence Server	Read Foundation Topics				
15. Cisco TelePresence Server	Review Key Topics				
15. Cisco TelePresence Server	Define Key Terms				
15. Cisco TelePresence Server	Complete memory tables in Appendix C for this chapter				

Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 15 in practice test software				
16. Cisco TelePresence Management Suite (TMS)	Read Foundation Topics				
16. Cisco TelePresence Management Suite (TMS)	Review Key Topics				
16. Cisco TelePresence Management Suite (TMS)	Define Key Terms				
16. Cisco TelePresence Management Suite (TMS)	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 16 in practice test software				
17. Cisco WebEx Solutions	Read Foundation Topics				
17. Cisco WebEx Solutions	Review Key Topics				
17. Cisco WebEx Solutions	Define Key Terms				
17. Cisco WebEx Solutions	Complete memory tables in Appendix C for this chapter				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 17 in practice test software				
18. Final Preparation	Read Chapter				
18. Final Preparation	Take practice test in study mode for all Book Questions in practice test software				
18. Final Preparation	Review all Key Topics in all chapters				
18. Final Preparation	Complete all memory tables from Appendix C				
18. Final Preparation	Take practice test in practice exam mode using Exam Bank #1 questions for all chapters				
18. Final Preparation	Take practice test in practice exam mode using Exam Bank #2 questions for all chapters				

Where are the Companion Content Files?

Thank you for purchasing this Premium Edition version of:

CCNA Collaboration CIVND 210-065 Official Cert Guide

The print version of this title comes with a disc of companion content. As an eBook reader, you have access to these files by following the steps below:

1. Go to **ciscopress.com/account** and log in.
2. Click on the "Access Bonus Content" link in the Registered Products section of your account page for this product, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps at left, please visit **ciscopress.com/contact** and select the "Site Problems/Comments" option. Our customer service representatives will assist you.

The Professional and Personal Technology Brands of Pearson

Addison Wesley · Cisco Press · IBM Press. · informIT · PEARSON IT Certification · Prentice Hall · que · SAMS · vmware PRESS